SYBEX *e*-trainer™ for Certification Success

CCNP™ Virtual Lab™ Version 1.01

The #1 Cisco Simulator

- Simulates A Real-World Network Environment
- Covers All Four CCNP Exams: Routing (640-503), Switching (640-504), Remote Access (640-505), and Support (640-506)
- Includes Dozens of Instructional Labs for Each Exam Plus Extensive Free-Form Configuration Options

SYBEX
25 YEARS OF PUBLISHING EXCELLENCE

Todd Lammle
William Tedder

Equip Yourself with the Knowledge and Skills You Need to Pass the CCNP Exams

CCNP™ Virtual Lab™

Routing (exam 640-503)

- IP addressing
- Configuring OSPF areas in a single area
- Interconnecting OSPF areas
- EIGRP
- Configuring, monitoring, troubleshooting, and scaling BGP

Switching (exam 640-504)

- Connecting the switch block
- Configuring 5000 and 1900 series switches with VTP and VLANs
- Working with Spanning Tree Protocol (STP)
- Using Spanning Tree with VLAN
- Setting up inter-VLAN routing
- Using Multi-Layer Switching (MLS)
- Implementing Hot Standby Routing Protocol (HSRP)
- Configuring multicast
- Planning and setting up access policies

Remote Access (exam 640-505)

- Using the Point-to-Point Protocol
- Setting up ISDN and dial-on-demand routing
- Working with the Cisco 700 series routers
- Configuring X.25 encapsulated links using LABP
- Working with Frame Relay

Support (exam 640-506)

- Diagnosing and troubleshooting common network problems
- Troubleshooting serial line and frame relay connectivity
- Troubleshooting ISDN
- Troubleshooting Novell IPX
- Troubleshooting switched ethernet

About the Developers:

Todd Lammle is one of today's foremost experts on LAN/WAN installation, configuration, and administration. He is president of GlobalNet Systems and author of the hugely popular *CCNA: Cisco Certified Network Associate Study Guide*, also from Sybex.

William Tedder, president of Interactive Designs Group Inc., is the person responsible for the intuitive, easy-to-use, and effective interface of the *CCNP Virtual Lab*. He holds graduate degrees in psychology and industrial design, and has been involved with computers and learning for more than 20 years.

Todd and Bill are the same team that brought you the **CCNA Virtual Lab**, another powerful certification tool from Sybex.

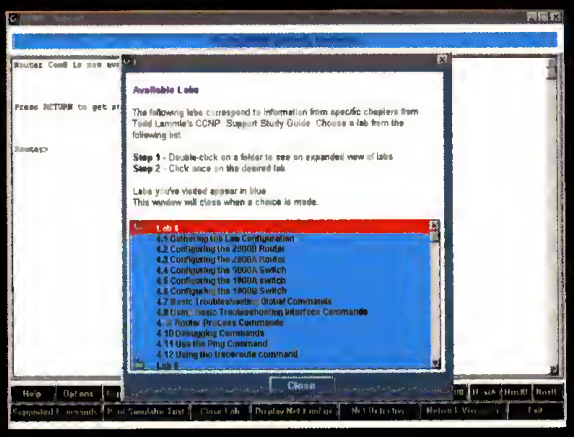
System Requirements

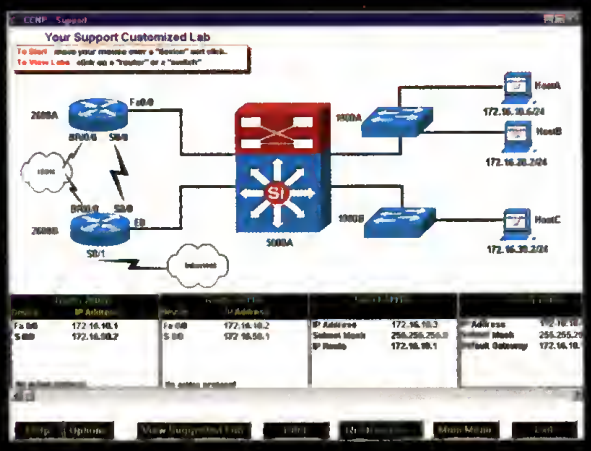
- Web browser and Internet connection
- Windows 95, Windows 98, Windows NT, Windows 2000
- 133MHz or faster Pentium
- 32MB RAM
- 2MB video card
- 7MB HD space
- 8X CD-ROM drive
- Mouse or other pointing device
- Small fonts

Get the Hands-on Experience You Need!

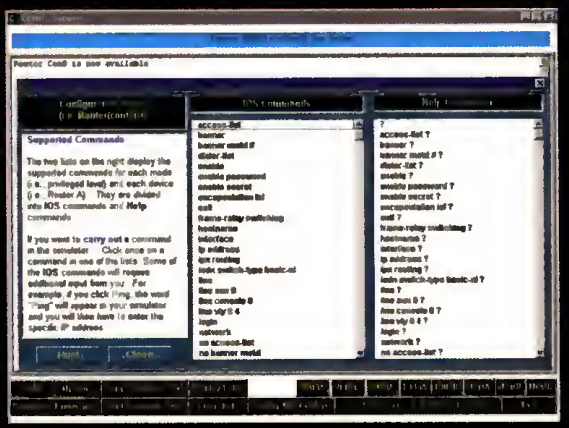
SYBEX'S *CCNP Virtual Lab* has been specially designed to help you make the most of your CCNP preparation efforts.

Learn Key Skills by Following Step-by-Step Instructional Labs

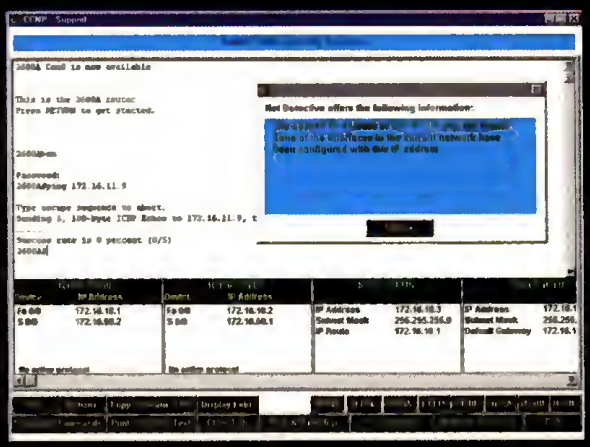




Develop Custom Labs that Focus on the Techniques and Scenarios that Matter Most to You



Practice with Hundreds of Router Commands



Use the Net Detective to Track Down—and Learn From—Your Mistakes

Visit the Sybex web sites (www.certification.sybex.com and www.sybexetrainer.com) for all your Cisco certification needs

The Leader in Certification

SYBEX®

SYBEX *e-trainer* for Certification Success

CCNP™ Virtual Lab™

The #1 Cisco Simulator

- Simulates A Real-World Network Environment
- Covers All Four CCNP Exams: Routing (640-503), Switching (640-504), Remote Access (640-505), and Support (640-506)
- Includes Dozens of Instructional Labs for Each Exam Plus Extensive Free-Form Configuration Options

SYBEX

25 YEARS OF PUBLISHING EXCELLENCE

Todd Lammle
William Tedder

CCNP™ Virtual Lab™

Todd Lammle
Bill Tedder

San Francisco • Paris • Düsseldorf • Soest • London

SYBEX®

Associate Publisher: Neil Edde
Contracts and Licensing Manager: Kristine O'Callaghan
Developmental Editor: Jeff Kellum
Editor: James A. Compton
Production Editor: Mae Lum
Technical Editor: Jim Taylor
Book Designer: Bill Gibson
Graphic Illustrator: Tony Jonick
Electronic Publishing Specialist: Adrian Woolhouse
Proofreaders: Laurie O'Connell, Mae Lum
Cover Design: Ingalls & Associates

Library of Congress Card Number: 2001091244

ISBN: 0-7821-2959-5

Manufactured in the United States of America

10 9 8 7 6 5 4 3

Software License Agreement

Important: Please read this license agreement carefully. This agreement between you, the end user, and Sybex Inc. is a legal document. If you do not agree to the terms of this license agreement, return the package, accompanying materials, and the CD-ROM disk(s) with proof of payment to the authorized dealer from whom you obtained it, for a full refund of the price you paid. Using the CD-ROM constitutes your acceptance of this license agreement.

1. GRANT OF LICENSE. In consideration of the purchase price paid by you, Sybex Inc. ("SYBEX") grants to you, as Licensee ("Licensee"), a single-user, non-exclusive, nontransferable, perpetual license to use this copy of its Software Program and related documentation (together the "Software") subject to the provisions of this agreement. SYBEX reserves all rights not expressly granted to Licensee.

2. PERMITTED USES. Licensee is granted the following rights in the Software:

(a) Right to Install and Use. You may install and use the Software on any hard disk drive of any single compatible computer that you own. However, you may not under any circumstances have the Software installed onto the hard drives of two or more computers at the same time, nor may you install the Software onto the hard drive of one computer and then use the original CD-ROM on another computer. If you wish to use the Software on a computer that is not the computer where the Software was first installed, you must either erase the Software from the first hard drive before you install it onto a second hard drive, or license an additional copy of the Software for each additional computer on which you want to use it.

(b) Right to Modify. You may not modify the Software and/or merge it into another computer program.

(c) Right to Transfer. You may not rent, lend, or lease this Software. However, you may transfer this license to use the Software to another party on a permanent basis by transferring this copy of the License Agreement, copy of the Software, and all documentation. You must, at the same time, either transfer to the other party or destroy all your copies of the Software. Such transfer of possession terminates your license from use. Such other party shall be licensed under terms of this agreement upon the acceptance of this agreement by the initial use of the Software. If you transfer the Software, you must remove the Software from your hard disk, and you may not retain any copies of the Software for your own use.

3. PROHIBITED USES. You may not, without written permission from us:

(a) Use, copy, modify, merge, or transfer copies of the Software or documentation except as provided by this agreement;

(b) Disassemble, decompile, or "unlock," reverse translate, or in any manner decode the Software for any reason; or

(c) Sub-license, lease, or rent the Software.

4. WARRANTY AND DISCLAIMER. SYBEX makes no warranties, express or implied, with respect to the Software or its performance, including, but not limited to, implied warranties of merchantability or fitness for a particular purpose. SYBEX warrants only that the software media is free of physical defects for a period of ninety (90) days from the date of purchase listed on the original invoice or bill of sale. SYBEX's total liability, and Licensee's sole remedy, under this warranty shall be limited to, at SYBEX's option, correction or replacement of the defective media. If you discover a defect in the media during this warranty period, you may obtain a replacement of identical format at no charge by sending the defective media, postage prepaid, with proof of purchase to: SYBEX Inc., Customer Service Department, 1151 Marina Village Parkway, Alameda, CA 94501. Phone: (510) 523-8233, Fax: (510) 523-2373. E-mail: info@sybex.com. Web: HTTP://WWW.SYBEX.COM.

After the 90-day period, you can obtain replacement media of identical format by sending us the defective disk, proof of purchase, and a check or money order for $10, payahle to SYBEX.

In no event shall SYBEX be liable for any special, indirect, or consequential damages arising out of or in connection with the use of or inability to use the Software or its contents even if advised of the possibility of such damage. (Some states do not allow the exclusion of implied warranties or liability for the incidental or consequential damages; therefore, the limitations stated above may not apply to Licensee.)

5. EXPORT CONTROLS. You agree to comply with all export laws and regulations of the United States as such laws and regulations may exist from time to time.

6. CANADIAN TRANSACTION. If you acquire this Software in Canada, you agree to the following: The Parties hereto have expressly required that the present agreement and any amendments be drawn up in the English language.

7. TERMINATION. This license and your right to use this Software automatically terminate if you fail to comply with any provisions of this agreement, destroy the copies of the Software in your possession, or voluntarily return the Software to us. Upon termination, you will destroy all copies of the Software and documentation. Otherwise, the restrictions on your rights to use the Software will expire upon expiration of the copyright of the Software.

8. MISCELLANEOUS PROVISIONS. This agreement will be governed by and constructed in accordance with the substantive laws of California, and not by the 1980 United Nations Convention on Contracts for the International Sale of Goods, as amended. This is the entire agreement between us relating to the contents of this package, and it supersedes any prior purchase order, communications, advertising, or representation concerning the contents of this package. No change or modification of this agreement will be valid unless it is in writing and is signed by us.

Please keep this Software License Agreement for future reference. If you have any questions about this agreement, write to us at 1151 Marina Village Parkway, Alameda, CA 94501, or call us at (510) 523-8233.

Contents

Getting Started

The Sybex CCNP Virtual Lab is not an exact duplicate of a network. What the Sybex CCNP does give you is the most realistic and sophisticated simulation-training tool on the market today. It was designed to follow along with Todd Lammle's best-selling CCNP Study Guide series published by Sybex (2001). Todd Lammle is an industry-recognized expert in the field of network certification.

Learning with the CCNP Virtual Lab

This product was mainly developed to be an instructional tool that you can use to learn how to configure a network. You start out configuring basic commands and proceed to more advanced topics in the labs. Along the way, you can put into practice what you read. As you interact with the simulator, you will learn what commands are appropriate at each mode, plus the effects they have on the configuration of your network.

It is important to read the four Sybex CCNP Study Guide books either before or during the configuration of the Virtual Lab, which will help explain the concepts of what the labs are trying to teach you.

You learn by doing, by interacting with a network in a safe environment. Because you're not practicing on "live" equipment, you don't have to worry about bringing down a network and affecting other users. This is your customized network that you build in any way you want. You can start over as many times as you like by removing any configuration(s) that you want, one command at a time, or erasing the entire configurations on the Cisco routers or switches.

Finally, people learn best when they can practice with realistic situations that model their actual working environment. That makes it easier for someone to transfer knowledge from an instructional setting to their real working environment, so feel free to customize your simulated network and model it after a live environment.

Security

For security purposes, we have included the StopCopy software protection program on the CCNP Virtual Lab. To help protect from individuals distributing pirated copies of CCNP Virtual Lab, you will need to register your product with Sybex before you can use the program. You can use this program on only one machine at a time, so in the following sections, we will show you how to install and uninstall the authorization license needed to run the program.

We realize that you may want to use this program on more than one computer. To do this, you will have to uninstall the authorization first, and then reinstall it when you install the CCNP Virtual Lab on the new computer. However, you cannot have the program installed on two computers simultaneously. This process takes seconds if you are connected to the Internet.

Installing Your Authorization License

When you install the CCNP Virtual Lab onto your hard drive, you will need to authorize your program to run. This is done through an Internet Authorization process. You will use the product ID number found on the front of your CD jewel case to authorize your program, and you must be connected to the Internet in order to perform the authorization procedure. If you cannot connect to the Internet, there is a manual method of gaining authorization. We will discuss how to do each below.

It is very important that you keep your product ID. Please be sure to keep the jewel case the number is on and write the product ID down so you don't lose it. If you lose the product ID, you will not be able to get authorization to run the program.

Internet Method

The product ID number on your CD jewel case allows you to activate one license. To install the authorization license using the Internet, follow these steps:

1. Make sure you are connected to the Internet.
2. On the Virtual Lab main menu, click the button that says "Install License."
3. You will then see three buttons. Click the button that says "Web Install."
4. You will be asked to enter your product ID number, which is located on the front of your CD jewel case.

5. Click the OK button. After a few seconds you will see a message telling you that you have completed a successful authorization. A license has been placed on your hard drive, in your application directory. You are now ready to use the program.

Manual Method

If you are unable to connect to the Internet when you want to authorize your program to run, you can do it manually by following these steps.

1. On the Virtual Lab main menu, click the button that says "Install License."
2. You will then see three buttons. Click the button that says "Manual Install."
3. A dialog box will appear, displaying a user number. There will also be a blank field that you will eventually fill in with an activation code. Call the Support Department at Sybex at 510-523-8233. Tell them which product you have, give them your user number and product ID, and they will give you an activation code.
4. Enter that activation code into the blank field in the dialog box and click the OK button.
5. A license will be placed on your hard drive, in your application directory. You are ready to use the program.

Removing Your Authorization License

You can use the CCNP Virtual Lab on only one computer at a time. If you want to use it on a different computer than is currently authorized, such as at work, you need to remove your authorization license from the first computer's hard drive. You can quickly remove your authorization. Once the authorization is removed, you can reinstall the CCNP Virtual Lab—and the authorization—on another computer. You can remove your authorization license either through the Internet or manually.

Internet Method

To remove your authorization license with this method, you will need to be connected to the Internet. The steps to this method follow:

1. On the Virtual Lab main menu, click the button that says "Remove License."
2. You will then see two buttons. Click the button that says "Web UnInstall."
3. You will be asked to enter your product ID number. Enter the product ID number from your jewel case. Click the OK button.
4. After a few seconds you will see a message telling you that you have completed a successful removal of your authorization. Your license has been placed back up on an Internet database.
5. When you want to run this program on another computer, follow the steps for installing your authorization via the Internet.

Manual Method

If you are unable to connect to the Internet and want to remove your authorization license, you can do it manually by following these steps.

1. On the Virtual Lab main menu, click the button that says "Remove License."
2. You will then see three buttons. Click the button that says "Manual Uninstall."
3. A dialog box will appear that will display a remove number. Call the Support Department at Sybex at 510-523-8233. Tell them which product you have and give them your remove number and product ID number, which is located on the CD jewel case.
4. When the technician tells you to proceed, click the OK button in the dialog box.
5. When you want to run this program on another computer, follow the steps for installing your authorization via the Internet.

If you use the manual method, you must call the Support Department at Sybex. They have to complete the manual process in order for your license to be available for installing on another computer. Once you see your remove number displayed, you can no longer use your program until you install the license again.

Should you decide to uninstall the CCNP Virtual Lab software from your PC at any time in the future, be sure to remove the license as well. To do this, click the Remove License button on the Main Menu screen. Failing to remove the license during an uninstall will result in operational errors when you attempt to run the software on a different computer.

Authorization Error Codes

For one reason or another, you may encounter an error code when you try to install your authorization or run the program. The following information will assist you in understanding and trying to figure out the source of the problem.

Code	Description
0	Your authorization file cannot be found. An error 0 can occur during verification of authorization when you try to go to the Network Visualizer screen from the main menu. Authorization was not found on your hard drive during verification. Either authorization has not been placed on the hard drive, it has been removed, or it has become corrupted. The likely cause of corruption is that a utility such as Norton Speed Disk has been run.

Code	Description
2	An authorization has already been activated on your computer.
3	This code can occur if the authorization on your hard drive has been corrupted. This can occur if it is tampered with or corrupted by another program such as a hard disk utility.
14	Database authorization file not found. An invalid product ID number was entered. Please try again.
15	Database authorization file not found. An invalid product ID number was entered. Please try again.
19	This code can occur if the authorization has not been activated on your hard drive. The authorization file actually exists on your hard drive, but in inactive form. You must be sure to activate the authorization file in order to use the product.
21	Database authorization file not found. An invalid product ID number was entered.
35	An invalid product ID code was entered. Please try again.
37	You are trying to remove an authorization from your hard drive but the program cannot find an activated file.
52	There are no more authorizations left to activate. The program comes with one license.
251	Connection to the server where you activated your authorization failed. Please try again.
252	Please check your Internet connection. You need to be connected to the Internet before you install or uninstall authorization.

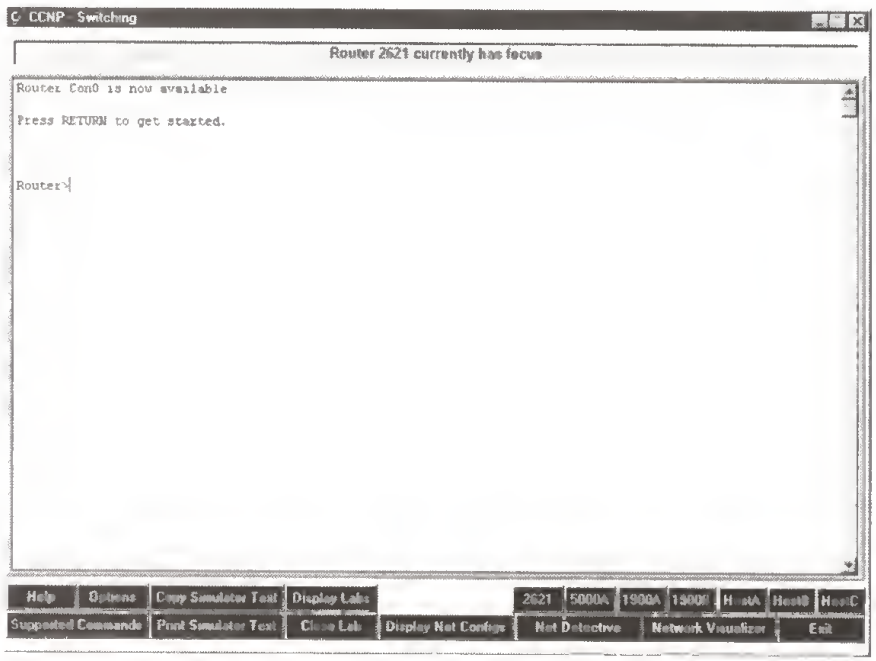
If at any time you have difficulty with the security feature of the CCNP Virtual Lab, please call Sybex Support at 510-523-8233 or e-mail them at support@sybex.com.

Getting Started with the CCNP Virtual Lab

This program allows you to work in four different simulated network environments, each focusing on one of the four CCNP exams. To start, click the button associated with the particular module: Routing, Switching, Support, or Remote

Access. You will see the Network Visualizer screen. Choose one of the routers or one of the switches by clicking the appropriate graphic on the screen that represents that device.

After you choose a device from the Network Visualizer screen, you will see a blinking cursor in the simulator field. Press Enter, and a prompt appears on the screen. You then have the choice of entering commands or opening a lab, as shown next.



Once you are in a simulator screen, you can go to another router or switch by clicking one of the buttons at the bottom of the screen instead of going back to the Network Visualizer screen.

Are There Any Restrictions to the CCNP Virtual Lab?

The Sybex CCNP Virtual Lab does not restrict you with any prompts or step-by-step instructions. You can follow along with the pre-determined labs, or you can interact with the simulator in a free-form fashion. Essentially, if you type in appropriate commands, you will see the fruits of your labor. Otherwise, you will see the same error responses that you would see while working with real routers.

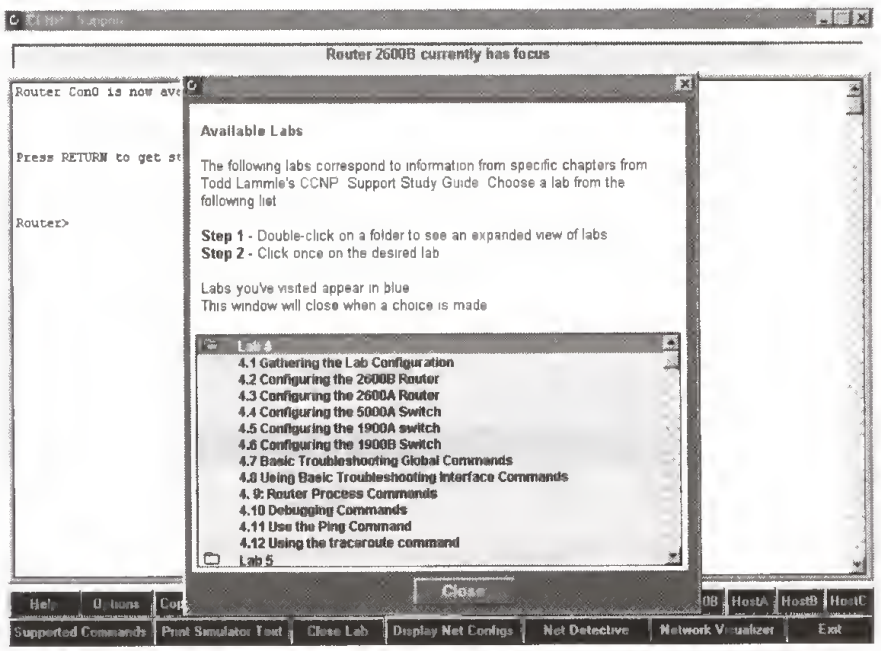
The Network Visualizer presents suggested IP addresses that you will enter as you use the labs. However, you can type in any IP address that you want, and it will show up in your customized lab. As long as you have IP addresses entered, a protocol is established, and the device interfaces are not shut down, you can communicate between the devices using your own IP addresses.

Commands Limited to the Labs

With a real router, you can enter hundreds of commands. The commands that can be carried out in this simulator are limited to those that are referenced in the labs. However, you still have a large set of commands available that allow you to completely configure your routers and have them communicate with each other.

Choosing a Lab

With the simulator field displayed, click the button at the bottom of the screen that says Display Labs. You will see several graphic folders with numbers to the right; these numbers represent the labs for the corresponding chapter from the specific Sybex Study Guide (for instance, if you are in the Routing module, the numbers correspond to the chapters in the *CCNP: Routing Study Guide*). Double-click a folder, and the individual labs are displayed, as shown below. Click once on a desired lab; the dialog box disappears, and the contents of the lab appear at the bottom of the screen.



Supported Commands

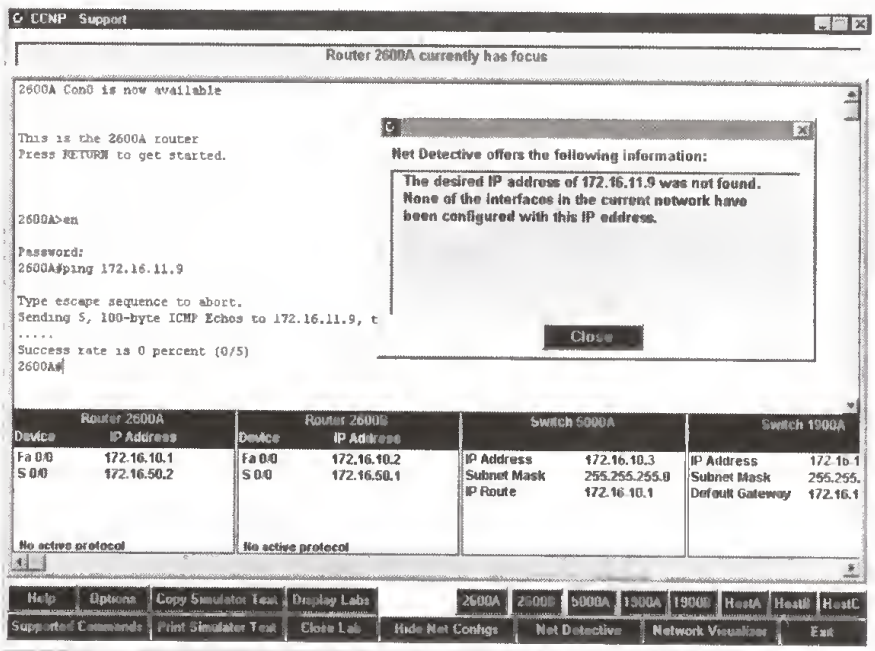
The supported commands are derived from the labs in the Sybex CCNP Virtual Lab. This does not include every command found in the CCNP Study Guides or all possible IOS commands from a router. However, there are a sufficient number of commands to allow you to fully configure the environment. Click the Supported Commands button to view those that are supported at each level.

Features of the CCNP Virtual Lab

The CCNP Virtual Lab has many features that make it easier to learn how to configure your simulated network environment. This section discusses each of these features in turn.

Net Detective

Net Detective assists you in diagnosing problems incurred while trying to communicate among the routers and switches. For example, if you are unsuccessful in trying to ping between routers 2501A and 2501C, Net Detective will provide a suggestion such as "Router 2501B s1 is shut down." You can access Net Detective by clicking the Net Detective button at the bottom of the screen.



Program Options

Clicking the Options button at the bottom of the screen opens a dialog box from which you can decide the following:

- If you want a lab displayed in a pop-up box or embedded below the simulator field. If your screen resolution is high enough, your lab can appear in a pop-up box, which can then be dragged to the bottom or top of your screen to create a full simulator field.
- If you want to save your configurations to a diskette instead of to your hard drive.

Printing and Copying

The CCNP Virtual Lab allows you to print your configuration as well as other components:

- You can print out labs.
- You can print the contents from the Help screens.
- You can print the list of supported commands.
- In the Network Visualizer, you can print out the suggested screen or the Your Customized Lab screen.

Additionally, you can copy the text from the simulator field so that you can paste it into another application.

Help Screens

There are now three distinct Help screens to assist you. When you click the Help button, a pop-up box displays a window with three tabs:

- Help
- Getting Started
- Lookups

Help

This will help you with any basic questions you may have about the program that address frequently asked questions and problems.

Getting Started

This section describes how to get started working within the program, how to learn using this program.

Lookups

This section allows users to look up passwords they may have set while working with the labs. If users forget their passwords, they can look them up here.

Navigation

The Virtual Lab offers several navigational options. While you are in the simulator field, you can use the F1 and F2 keys to scroll up and down an open lab. When you click in the lab itself, you can use the following keys for navigation: Page Down, Page Up, Down Arrow, Up Arrow, Ctrl+Home (to go to the top of the screen), and Ctrl+End (to go to the bottom of the screen).

How to Use the CCNP Virtual Lab

When you first start the program and go to the simulator field, you will see a blinking cursor. Press the Enter key to get started. You should then see a prompt. If you click anything outside of the simulator field (such as another program), you will have to click within the simulator field so that it can gain *focus*. When in doubt, click within the simulator field; a cursor should then appear at the end of the last line of text. The exception to this is when you are viewing a lab.

Cursor Movement and the Mouse

When you scroll your simulator field, moving the cursor off the scroll will cause the simulator prompt (cursor) to "snap" back to the last line in the simulator. As long as you do not move your cursor off of the scrolling portion of the simulator field, the cursor will not snap back. Remember that you can always copy and/or print text from the simulator field.

Scrolling the Simulator Field

In the simulator field, you can view any information that has scrolled out of view. Simply place your cursor in the scrolling region of the simulator field and move to the desired location. Notice that you will not be able to highlight and delete text. However, you can copy or print the text in the simulator field.

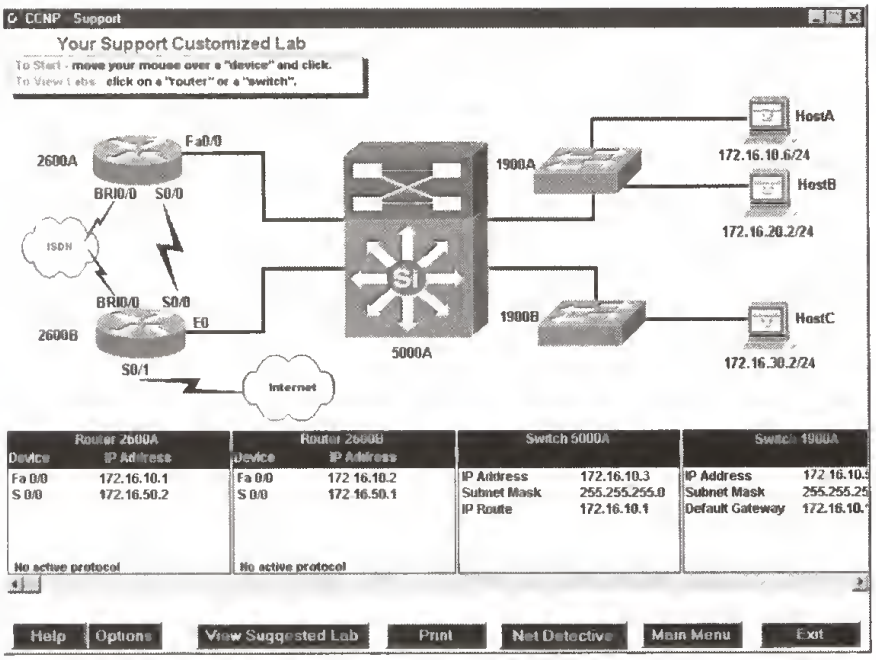
Saving Information

It will not be uncommon for you to work with this simulator over a span of several days. Any information that you enter, as it relates to configuring the routers, can be saved. In Privileged mode (at the Router# prompt), the command `copy run start` can be typed in, and after you press Enter, the configuration for that router will be saved to a text file. The switches save their configuration automatically to NVRAM, just like real switches.

If you accidentally delete the text file associated with configuration settings for a router, nothing will happen to the program. However, you will have to start over and reconfigure your router or switch. It would be like starting up with nothing in your NVRAM.

Interacting with Network Visualizer

The Virtual Lab allows you to view two lab diagrams. When you click the Network Visualizer button on the Virtual Lab's main screen, you will see Your Customized Lab, which displays the configuration information that you enter (as shown in the following sample screen).



On this screen, you can click the View Suggest Lab button to view the Suggested Lab diagram, which presents the suggested network settings as they relate to your connected network. It also displays the suggested IP addresses that are referred to in the various labs.

If you want to observe your progress as you configure the routers, you can quickly see where you are by examining Your Customized Lab. More important, if you're having trouble communicating between routers, this diagram may provide you with important information as to why communication is not taking place. You can also use Net Detective to assist you in diagnosing a problem, as discussed earlier.

Using Supported Commands

The labs in the Virtual Lab are directly associated with various chapters from the four Sybex CCNP Study Guides. As you start looking at the bigger picture in terms of how everything is related, you may want to know about the availability of commands for each mode.

Depending on which mode you are in (User, Privileged, Configuration, or Interface), the Supported Commands feature provides a list of all commands available for that mode. The commands are divided into IOS commands and help commands. This saves time if you are not using the labs and want to quickly look up available commands for a specific mode. For example, there are many `show` commands dispersed throughout the labs. If you want to see all available IOS `show` commands or all the Help `show` commands (i.e., `show ip ?`) for a mode, this allows you to see all of them without having to go through all the labs trying to locate all `show` commands. By using Supported Commands, you will quickly see which commands are available.

Automatically Performing the Commands

As you view the list of supported commands, you can have the program perform a command by clicking once on the item from the list. In this way, for example, you can rapidly perform all the Show commands and view the output on the screen.

Some of the commands will not automatically execute because you need to complete the command by entering additional information. An example would be when you click the word *ping*. It will appear on the screen, but no action will take place because you need to finish the command by entering an IP address.

Printing Field Content

You can print the contents of the simulator field by clicking the Print button. This allows you to have a hard copy of your interaction with the simulator. You can then examine what you have typed and the effects it has had on the simulator and the configuration of routers and switches.

Closing a Lab

If you want to remove a lab from the lower part of the screen and return to a larger view of the router simulator, click the Close Lab button at the bottom of the screen. You will not lose any information typed into the simulator field. The text will readjust and fill up the larger screen. If you have chosen to view a lab in a pop-up dialog box, you can close the lab by clicking the Close Lab button or by clicking the X in the right-hand corner of the pop-up dialog box.

Pressing the Tab Key to Finish Commands

Just as you can with a real router, you can type in a partial command and press the Tab key to see the full command on the next line. Then press your Enter key to execute the command.

Starting Over

You can completely remove your startup configuration from any device (i.e., router or switch). For each router, type in the command `erase start` and press the Tab key to see the entire command, or press Enter. This will reinitialize your configuration files. At this point, if you want to remove the configuration that you have existing in memory, use the `reload` command. To remove your configuration from a switch, you would invoke the command `delete nvram` while you are in privileged mode.

Shortcut Commands

A number of shortcut commands are available in this simulator. For example, if you want to enter the command `show startup-config`, you can type in **sh start**. Another example is if you want to see a history of commands that you have entered into the program. The longhand command is `Show History`, but you can also type in **sh history**, **sh hist**, or **sh his**.

Ping or Telnet Not Working

If you can ping, you can telnet, and vice versa. Here are some things to check for if you cannot communicate with another router:

1. Make sure that all interfaces between the two points of communication have IP addresses.
2. Make sure that all interfaces between the two points of communication are not shut down (remember to do a **no shut** after entering IP addresses).
3. Make sure that you have established a routing protocol—either through a static route, rip route, or IGRP route.

Be sure to use Net Detective to help you diagnose problems.

Conventions Used in This Booklet

The labs in this booklet are numbered to correspond to the chapters in the appropriate Sybex CCNP Study Guide so that you can follow along with ease. The commands within the labs will appear in lowercase `code font`, and in lowercase **bold text** when it is user input, unless otherwise noted. When a given command is followed by a period, please note that the period is not part of the command but part of the punctuation, as seen in this example: Log in by typing **en** or **enable**. For the command to work, you would not type in the period. Also, there are many notes in this booklet that offer tidbits of information, reminders, and warnings. Generally, they are positioned below the material to which they refer.

Summary

In this introduction, you learned the basics of the CCNP Virtual Lab. You should have a good understanding of the product's benefits as well as the limitations of the simulator. It's a great product, and it is the only one on the market that lets you practice virtually, on your own PC, whenever you need to practice configuring routers and switches.

Check out the RouterSim Web site for upgrade information for all Virtual Lab products. Just go to `www.routersim.com/Sybex/upgrade.htm`. Good luck!

Please note that, even after the software has been installed, the CD must be present in the drive in order for the software to run. If you encounter problems with the CD, please read the `readme.txt` file on the root of the CD for support information.

Module 1: CCNP Routing Suggested Labs

These labs are designed to help you prepare for and pass the Cisco CCNP Routing exam (640-503). The labs follow the new Sybex *CCNP: Routing Study Guide*.

These labs can work in conjunction with any study guide or even as a stand-alone product. However, we recommend that you read the Sybex *CCNP: Routing Study Guide*, since all commands used in these labs are discussed and described in the book.

The following labs are covered in the Routing module and are referenced from the *CCNP: Routing Study Guide*:

- Chapter 3: IP Addressing
- Chapter 4: OSPF Areas
- Chapter 5: Interconnecting OSPF Areas
- Chapter 6: IGRP and EIGRP
- Chapter 8: Configuring Basic BGP

Labs from Chapter 3: IP Addressing

These labs will describe how to connect two Cisco routers together with serial connections without using an IP address. This is a Cisco proprietary feature called IP unnumbered.

IP unnumbered is used to connect point-to-point serial links together without using an IP subnet. It is typically used when you do not have many subnets to spare or you are connecting discontiguous networks together.

Lab 3.1: Configuring IP Unnumbered

This section demonstrates the `ip unnumbered` command as well as using the loopback interface of Cisco's IOS for diagnostic purposes. It's a good idea to set the passwords on each router for practice, but that is not required in this lab. Configure the `ip unnumbered` command between routers 2501B and 2501C. Use the following IP addresses:

Router	IP Address
2501A	Int s0:172.16.20.1/24
	Int e0:172.16.10.1/24
2501B	Int s0: 172.16.20.2/24
	Int e0: 172.16.30.1/24
	Int loopback 0: 172.16.80.1/24
2501C	Int e0: 172.16.50.1/24
	Int loopback 0: 172.16.100.1/24

Switch	IP Address
1900A	172.16.10.2/24
1900B	172.16.30.2/24
1900C	172.16.50.2/24

Remember that the switches do not have an IP address configured on any interface; instead, the IP address is set in global configuration mode only.

1. Go to router 2501A and press Enter; then configure the hostname.

```
Router> ena
Router#config t
Router(config)#hostname 2501A
2501A(config)#
```

2. Configure the IP addresses on 2501A.

```
2501A(config)#int s0
2501A(config-if)#ip address 172.16.20.1 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#int e0
2501A(config-if)#ip address 172.16.10.1 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#^z
2501A#copy run start
```

3. Go to router 2501B and press Enter; then configure the hostname.

```
Router> ena
Router#config t
Router(config)#hostname 2501B
2501B(config)#
```

4. Configure the IP addresses on the 2501B router. Both serial interfaces on the 2501B router are DCE connections and need clock rates. Do not put an IP address on the serial 1 interface.

```
2501B(config)#int s0
2501B(config-if)#ip address 172.16.20.2 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#clock rate 64000
2501B(config-if)#int e0
2501B(config-if)#ip address 172.16.30.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#int s1
2501B(config-if)#clock rate 64000
```

5. Configure a loopback interface on 2501B with an IP address of 172.16.80.1 and a 24-bit subnet mask.

```
2501B(config-if)#int loopback0
2501B(config-if)#ip address 172.16.80.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#^z
2501B#copy run start
```

6. Configure the hostname and IP address on the 2501C router. Do not add an IP address to serial 0.

```
Router> ena
Router#config t
Router(config)#hostname 2501C
2501C(config)#int e0
2501C(config-if)#ip address 172.16.50.1 255.255.255.0
2501C(config-if)#no shut
```

7. Configure a loopback interface on 2501C with an IP number of 172.16.100.1 and a 24-bit subnet mask. The configuration of 2501C is as follows:

```
2501C(config-if)#int loopback0
2501C(config-if)#ip address 172.16.100.1 255.255.255.0
2501C(config-if)#no shut
2501C(config-if)#^z
2501C#copy run start
```

8. Configure the serial interfaces of routers 2501B and 2501C with the `ip unnumbered` command. Use interface loopback 0 for the supported interface.

   For 2501B, here is the configuration:

```
2501B(config-if)#int s1
2501B (config-if)#ip unnumbered loopback0
2501B (config-if)#no shut
```

   For 2501C, here is the configuration:

```
2501C (config-if)#int s0
2501C (config-if)#ip unnumbered loopback0
2501C (config-if)#no shut
```

9. Configure all routers to run RIP version 2. Since you have a contiguous network, you need to make sure that RIP does not summarize on classful boundaries. The `no auto-summary` command is necessary or a network loop will occur because network 172.16.0.0/24 will be advertised from 2501C and 2501B, which is wrong.

   For 2501A, here is the configuration:

```
2501A(config-if)#exit
2501A(config)#router rip
2501A(config-router)#version 2
2501A(config-router)#no auto-summary
2501A(config-router)#network 172.16.0.0
```

   For 2501B, here is the configuration:

```
2501B(config-if)#exit
2501B(config)#router rip
```

```
2501B(config-router)#version 2
2501B(config-router)#no auto-summary
2501B(config-router)#network 172.16.0.0
```

For 2501C, here is the configuration:

```
2501C(config-if)#exit
2501C(config)#router rip
2501C(config-router)#version 2
2501C(config-router)#no auto-summary
2501C(config-router)#network 172.16.0.0
```

10. Check the routing tables with the `show ip route` command on router 2501A.

```
2501A(config-router)#exit
2501A(config)#exit
2501A#show ip route
```

11. Check the routing tables with the `show ip route` command on router 2501B.

```
2501B(config-router)#exit
2501B(config)#exit
2501B#show ip route
```

12. Check the routing tables with the `show ip route` command on router 2501C.

```
2501C(config-router)#exit
2501C(config)#exit
2501C#show ip route
```

13. To test your configuration, from 2501A, ping 172.16.100.1 and 172.16.50.1.
14. To further test your configuration, from 2501C, ping 172.16.10.1.
15. Ping from all three hosts to all configured interfaces.
16. You can also configure the 1900A, B, and C switches with IP addresses and ping the switches from the routers.

For the 1900A switch, here is the configuration:

```
>ena
#config t
(config)#hostname 1900A
1900A(config)#ip address 172.16.10.2 255.255.255.0
```

For the 1900B switch, here is the configuration:

```
>ena
#config t
(config)#hostname 1900B
1900B(config)#ip address 172.16.30.2 255.255.255.0
```

For the 1900C switch, here is the configuration:

```
>ena
#config t
(config)#hostname 1900C
1900C(config)#ip address 172.16.50.2 255.255.255.0
```

17. You should now be able to ping all hosts, routers, and switches.

Labs from Chapter 4: OSPF Areas

The labs in this section show how to configure Cisco routers with OSPF in a single area. These labs assume that you have configured the IP addresses from lab 3. However, you are going to assign a subnet (172.16.40.0/24) between routers 2501B and 2501C and disable `ip unnumbered` between the routers. This section includes the following lab exercises:

- Lab 4.1: Configuring OSPF neighbors
- Lab 4.2: Verifying OSPF operation

Lab 4.1: Configuring OSPF Neighbors

This lab will show you how to configure simple OSPF operation between Cisco routers and how to verify this configuration.

Configure all router interfaces to be in OSPF area 0.

1. Configure the network between 2501A and 2501B and the Ethernet interface on 2501A. The wildcard bits are all 0, indicating that the network address must match up exactly.

```
2501A#config t
2501A(config)#router ospf 100
2501A(config-router)#network 172.16.20.1 0.0.0.0 area 0
2501A(config-router)#network 172.16.10.1 0.0.0.0 area 0
2501A(config-router)#^Z
2501A#
```

The wildcard configuration shown above configures individual interfaces into area 0.

2. Configure the 2501B router for OSPF. Assign all interfaces to Area 0. First, assign IP address 172.16.40.1/24 to interface s1 and disable the `ip unnumbered` command.

```
2501B#config t
2501B(config)#int s1
2501B(config-if)#ip address 172.16.40.1 255.255.255.0
2501B(config-if)#no ip unnumbered loopback 0
```

Since all interfaces are in the same OSPF area, you could alternatively configure the router with one OSPF `network` command, using the wildcard bits, instead of by assigning addresses to individual interfaces.

```
2501B(config-if)#router ospf 101
2501B(config-router)#network 172.16.0.0 0.0.255.255
  area 0
2501B(config-router)#^Z
2501B#
```

In the wildcard used above, the 0s indicate that the first two octets must match up exactly, but the 255s indicate that the last two bytes can be any value. The wildcard 0.0.255.255, then, indicates that any subnet and host bits associated with 172.16.0.0 will be in OSPF area 0.

3. Configure the 2501C router for OSPF. Before you can do that, however, you must first assign serial 0 to 172.16.40.2/24 and remove the `ip unnumbered` command.

```
2501C#config t
2501C(config)#int s0
2501C(config-if)#ip address 172.16.40.2 255.255.255.0
2501C(config-if)#no ip unnumbered loopback0
2501C(config-if)#router ospf 102
2501C(config-router)#network 172.16.40.0 0.0.0.255 area 0
2501C(config-router)#network 172.16.50.0 0.0.0.255 area 0
2501C(config-router)#^Z
2501C#
```

Notice in the configuration of 2501C that you used a different wildcard mask. This mask tells the router that subnets 40 and 50 are in area 0.

Even though you configured the three routers three different ways, each way is absolutely correct.

Please see the Sybex *CCNP: Routing Study Guide* for a complete explanation of areas and wildcard bits.

Lab 4.2: Verifying OSPF Operation

This lab demonstrates the commands used to verify OSPF on a Cisco router. To verify your configuration, take the following three steps.

1. Execute a `show ip ospf neighbor` command from each router. What are the results?
2. Execute a `show ip route` command to verify that all routes are being learned by all other routers.
3. Test the network by pinging all devices.

Labs from Chapter 5: Interconnecting OSPF Areas

The labs in this section show how to configure OSPF in multiple areas. To begin, erase any configuration on the routers. If you have completed Labs 3 and 4, the router configurations you did there need to be deleted. This section includes the following lab exercises:

- Lab 5.1: Deleting the router configurations
- Lab 5.2: Configuring the routers with IP addresses
- Lab 5.3: Enabling the OSPF Process
- Lab 5.4: Configuring OSPF Neighbors
- Lab 5.5: Verifying OSPF Operation

Lab 5.1: Deleting the Router Configurations

In this section, you will delete and verify that you have no configuration on your routers.

1. Go to the 2501A router and type **erase startup-config**, and then reload the router.

   ```
   2501A>ena
   2501A#erase startup-config
   2501A#reload
   ```

2. Go to the 2501B router and type **erase startup-config**, and then reload the router.

   ```
   2501B>ena
   2501B#erase startup-config
   2501B#reload
   ```

3. Go to the 2501C router and type **erase startup-config**, and then reload the router.

   ```
   2501C>ena
   2501C#erase startup-config
   2501C#reload
   ```

In the above example, notice that you did not delete the switch configurations, a step that is not important to do for this lab. However, if you wish to delete the configurations on the switches, use the `delete nvram` command.

Lab 5.2: Configuring the Routers with IP Addresses

In this lab, you will configure the routers with IP addresses. Before you continue on with the following labs, configure the routers and switches with the following configuration:

Router	IP Address
2501A	int s0:172.16.20.1/24
	int e0:172.16.10.1/24

Router	IP Address
2501B	int s0: 172.16.20.2/24
	int e0: 172.16.30.1/24
	int s1: 172.16.40.1/24
2501C	int e0: 172.16.50.1/24
	int s0: 172.16.40.2/24

Switch	IP Address
1900A	172.16.10.2/24
1900B	172.16.30.2/24
1900C	172.16.50.2/24

Remember that the switches do not have an IP address configured on any interface; instead, the IP address is set in global configuration mode only.

1. Go to router 2501A and press Enter; then configure the hostname and IP addresses.

```
Router>ena
Router#config t
Router(config)#hostname 2501A
2501A(config)#int s0
2501A(config-if)#ip address 172.16.20.1 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#int e0
2501A(config-if)#ip address 172.16.10.1 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#^z
2501A#copy run start
```

2. Go to router 2501B and press Enter; then configure the hostname and IP addresses. Remember that both serial interfaces on 2501B are DCE connections and need clock rates.

```
Router>ena
Router#config t
Router(config)#hostname 2501B
2501B(config)#int s0
2501B(config-if)#ip address 172.16.20.2 255.255.255.0
2501B(config-if)#no shut
```

```
2501B(config-if)#clock rate 64000
2501B(config-if)#int e0
2501B(config-if)#ip address 172.16.30.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#int s1
2501B(config-if)#ip address 172.16.40.1 255.255.255.0
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
2501B(config-if)#^z
2501B#copy run start
```

3. Configure the hostname and IP address on Router 2501C router.

```
Router>ena
Router#config t
Router(config)#hostname 2501C
2501C(config)#int e0
2501C(config-if)#ip address 172.16.50.1 255.255.255.0
2501C(config-if)#no shut
2501C(config-if)#int s0
2501C(config-if)#ip address 172.16.40.2 255.255.255.0
2501C(config-if)#no shut
2501C(config-if)#^z
2501C#copy run start
```

Lab 5.3: Enabling the OSPF Process

This lab shows you how to enable the OSPF process. To turn on OSPF on a router, use the **router ospf process-number** command. The process number can be any number and is only locally significant.

1. Enable OSPF process 100 on 2501A.

```
2501A#config t
2501A(config)#router ospf 100
2501A(config-router)#^Z
```

2. Enable OSPF process 101 on 2501B.

```
2501B#config t
2501B(config)#router ospf 101
2501B(config-router)#^Z
2501B#
```

3. Enable OSPF process 102 on 2501C.

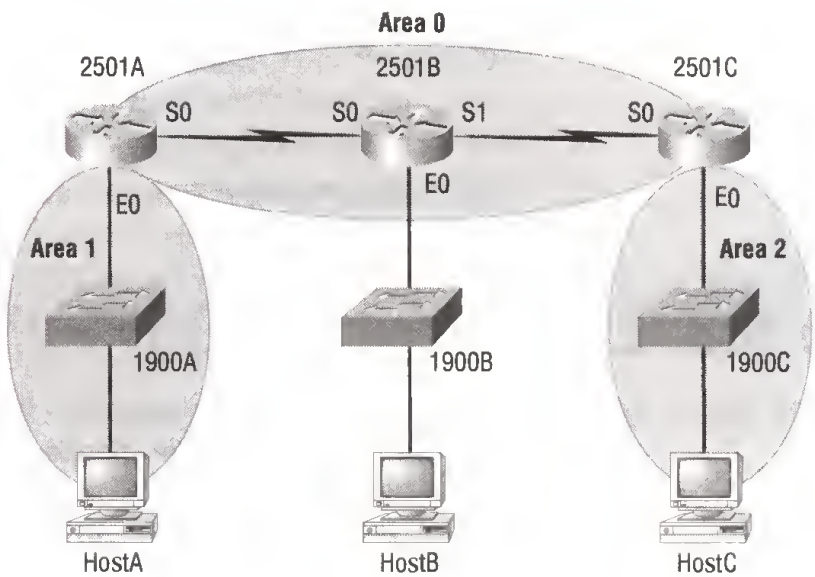
```
2501C#config t
2501C(config)#router ospf 102
2501C(config-router)#^Z
2501C#
```

Lab 5.4: Configuring OSPF Neighbors

This lab will show you how to configure OSPF neighbors. The OSPF areas you are going to assign are as follows:

- Area 0: Serial connection between 2501A and 2501B, serial connection between 2501B and 2501C and Ethernet 0 in 2501B.
- Area 1: Ethernet interface on 2501A
- Area 2: Ethernet interface on 2501C

The configuration will look like this:



1. Configure the network between 2501A and 2501B and the Ethernet interface on 2501A. Assign serial 0 to Area 0 and Ethernet 0 to Area 1. (To understand the wildcard bits, please read Chapters 4 and 5 of the Sybex *CCNP: Routing Study Guide*.)

```
2501A#config t
2501A(config)#router ospf 100
2501A(config-router)#network 172.16.20.1 0.0.0.0 area 0
```

```
2501A(config-router)#network 172.16.10.1 0.0.0.0 area 1
2501A(config-router)#^Z
2501A#
```

2. Configure the 2501B router for OSPF. Assign all interfaces to Area 0. Since all interfaces are in the same OSPF area, there are two ways to configure OSPF for all interfaces in 2501B. Here is the first way:

```
2501B#config t
2501B(config)#router ospf 101
2501B(config-router)#network 172.16.20.2 0.0.0.0 area 0
2501B(config-router)#network 172.16.30.1 0.0.0.0 area 0
2501B(config-router)#network 172.16.40.1 0.0.0.0 area 0
2501B(config-router)#^Z
2501B#
```

Here is the second way:

```
2501B(config)#router ospf 101
2501B(config-router)#network 172.16.0.0 0.0.255.255
  area 0
```

3. Configure the 2501C router for OSPF. Assign interface s0 to Area 0 and Ethernet 0 to Area 2.

```
2501C#config t
2501C(config)#router ospf 102
2501C(config-router)#network 172.16.40.0 0.0.0.255 area 0
2501C(config-router)#network 172.16.50.1 0.0.0.0 area 2
2501C(config-router)#^Z
2501C#
```

Lab 5.5: Verifying OSPF Operation

This short lab will provide you with the commands necessary to verify the configuration on a Cisco router. To verify your configuration, take the following three steps:

1. Execute a `show ip ospf neighbor` command from each router. What are the results?
2. Execute a `show ip route` command to verify that all routes are being learned by all other routers.
3. Test the network by pinging all devices.

Labs from Chapter 6: IGRP and EIGRP

The labs in this section will show you how to configure Enhanced IGRP on a Cisco internetwork using Variable Length Subnet Masks (VLSM). Before this series of labs can be completed, delete the configurations from all routers and switches.

This section includes the following lab exercises:

- Lab 6.1: Deleting the router and switch configurations
- Lab 6.2: Configuring the routers with IP addresses
- Lab 6.3: Enabling the EIGRP process
- Lab 6.4: Verifying EIGRP operation

Lab 6.1: Deleting the Router and Switch Configurations

In this section, you will delete the configuration on your routers and switches.

1. Go to the 2501A router and type **erase startup-config**, and then reload the router:

```
2501A>ena
2501A#erase startup-config
2501A#reload
```

2. Go to the 2501B router and type **erase startup-config**, and then reload the router:

```
2501B>ena
2501B#erase startup-config
2501B#reload
```

3. Go to the 2501C router and type **erase startup-config**, and then reload the router:

```
2501C>ena
2501C#erase startup-config
2501C#reload
```

4. Go to the 1900A switch and type **delete nvram**:

```
1900A>ena
1900A#delete nvram

Reset switch configuration to factory default? y
```

5. Go to the 1900B switch and type **delete nvram**:

```
1900B>ena
1900B#delete nvram

Reset switch configuration to factory default? y
```

6. Go to the 1900C switch and type **delete nvram**:

```
1900C>ena
1900C#delete nvram

Reset switch configuration to factory default? y
```

Lab 6.2: Configuring the Routers with IP Addresses

Variable Length Subnet Masks (VLSM) allows you to assign IP addresses on a granular basis. In this lab, you will configure subnet masks with only two IP addresses for the WAN links.

Use the following network address: 192.168.10.0. Our network diagram has two point-to-point WAN links that need only two IP addresses and three LANs that need three IP addresses each.

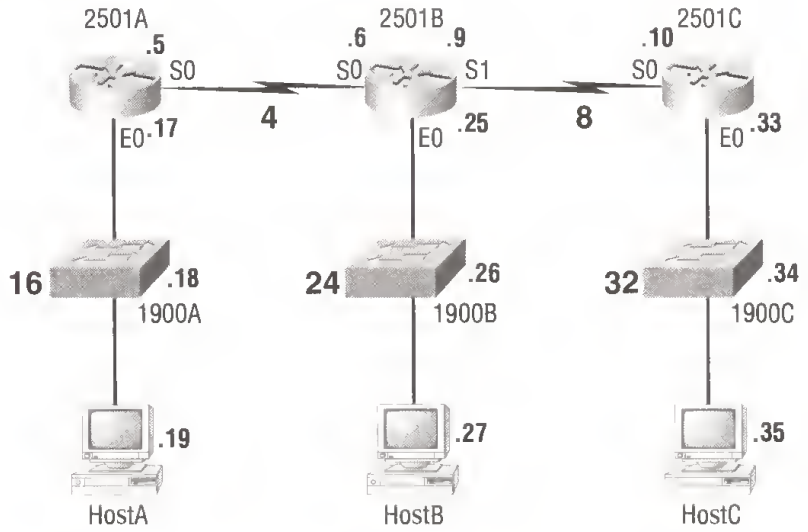
For the two WANs, use the following two subnets:

192.168.10.4/30 (valid hosts are 5 and 6)
192.168.10.8/30 (valid hosts are 9 and 10)

For the three LANs, use the following three subnets:

192.168.10.16/29 (valid hosts are 17–22)
192.168.10.24/29 (valid hosts are 25–30)
192.168.10.32/29 (valid hosts are 33–38)

Here is our network with the IP addresses assigned to the routers and switches:



1. Configure the hostname and IP addresses for 2501A.

```
Router>ena
Router#config t
Router(config)#hostname 2501A
2501A(config)#int s0
2501A(config-if)#ip address 192.168.10.5
  255.255.255.252
2501A(config-if)#no shut
2501A(config-if)#int e0
2501A(config-if)#ip address 192.168.10.17
  255.255.255.248
2501A(config-if)#no shut
2501A(config-if)#^z
2501A#copy run start
```

2. Go to the 2501B router and configure the hostname and IP addresses. Remember that both serial interfaces on 2501B are DCE connections and need clock rates.

```
Router>ena
Router#config t
Router(config)#hostname 2501B
2501B(config)#int s0
2501B(config-if)#ip address 192.168.10.6
  255.255.255.252
2501B(config-if)#no shut
```

```
2501B(config-if)#clock rate 64000
2501B(config-if)#int e0
2501B(config-if)#ip address 192.168.10.25
  255.255.255.248
2501B(config-if)#no shut
2501B(config-if)#int s1
2501B(config-if)#ip address 192.168.10.9
  255.255.255.252
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
2501B(config-if)#^z
2501B#copy run start
```

3. Configure the hostname and IP addresses on the 2501C router.

```
Router>ena
Router#config t
Router(config)#hostname 2501C
2501C(config)#int e0
2501C(config-if)#ip address 192.168.10.33
  255.255.255.248
2501C(config-if)#no shut
2501C(config-if)#int s0
2501C(config-if)#ip address 192.168.10.10
  255.255.255.252
2501C(config-if)#no shut
2501C(config-if)#^z
2501C#copy run start
```

4. Configure the 1900A switch with hostname and IP address, including the default gateway.

```
>ena
#config t
(config)#hostname 1900A
1900A(config)#ip address 192.168.10.18 255.255.255.248
1900A(config)#ip default-gateway 192.168.10.17
```

5. Configure the 1900B switch with hostname and IP address, including the default gateway.

```
>ena
#config t
(config)#hostname 1900B
1900B(config)#ip address 192.168.10.26 255.255.255.248
1900B(config)#ip default-gateway 192.168.10.25
```

6. Configure the 1900C switch with hostname and IP address, including the default gateway.

```
>ena
#config t
(config)#hostname 1900C
1900C(config)#ip address 192.168.10.34 255.255.255.248
1900C(config)#ip default-gateway 192.168.10.33
```

7. Verify your configurations by pinging your directly connected neighbors and using the **show cdp neighbors** command. You will not be able to ping to remote neighbors until you have a routing protocol configured.

Lab 6.3: Enabling the EIGRP Process

This section demonstrates enabling EIGRP on the three routers. Remember that EIGRP is a classless protocol, which means that it sends subnet mask information with the routing updates. This allows you to use a VLSM design on your network. However, EIGRP is a classful routing protocol, which means that you just advertise network 192.168.10.0 and let the routing protocol advertise the subnets. You do not configure subnet information within the EIGRP process.

One more thing you need to keep in mind when configuring EIGRP is that Autonomous System (AS) numbers must be configured. An AS can be any number from 1 to 65534, but remember that all routers must use the same AS number if they want to share routing information.

1. Configure router 2501A with EIGRP using AS 10:

```
2501A#config t
2501A(config)#router eigrp 10
2501A(config-router)#network 192.168.10.0
```

2. Configure router 2501B with EIGRP using AS 10:

```
2501B#config t
2501B(config)#router eigrp 10
2501B(config-router)#network 192.168.10.0
```

3. Configure router 2501C with EIGRP using AS 10:

```
2501C#config t
2501C(config)#router eigrp 10
2501C(config-router)#network 192.168.10.0
```

That is all there is to configuring basic EIGRP routing on a Cisco internetwork.

Lab 6.4: Verifying EIGRP Operation

It is important to understand how to verify the EIGRP routing protocol running on your network.

1. On each router, verify the routing table with the `show ip route` command. However, you can also type in **`show ip route eigrp`** to see only the routes found by EIGRP.
2. On each router, use the **`show ip eigrp neighbor`** command to see the EIGRP neighbor table.
3. On each router, use the **`show ip eigrp topology`** command to see the EIGRP topology table.
4. Ping from each router to each router, switch, and host to verify IP connectivity.

Labs from Chapter 8: Configuring Basic BGP

These labs will demonstrate a very simple configuration of BGP over two routers in different autonomous systems. Before this series of labs can be completed, delete the configurations from all routers and switches, using the same steps as in Lab 6.1.

This section includes the following lab exercises:

- Lab 8.1: Assigning IP addresses to the router and switches
- Lab 8.2: Enabling BGP on each router
- Lab 8.3: Verifying BGP configurations

The labs associated with this lesson correspond directly with Chapter 8 of the Sybex *CCNP: Routing Study Guide*. However, these labs assume knowledge from Chapter 7 as well.

Lab 8.1: Assigning IP Addresses to the Router and Switches

The following lab shows how to configure your routers and switches with IP addresses.

1. For router 2501A, configure the hostname, IP addresses, and loopback IP address (which will become the advertised BGP Router ID):

```
Router>enable
Router#config t
Router(config)#hostname 2501A
2501A(config)#int s0
2501A(config-if)#ip address 172.16.11.1 255.255.255.0
2501A(config-if)#bandwidth 64
2501A(config-if)#no shut
2501A(config-if)#in e0
2501A(config-if)#ip address 172.16.15.1 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#int loopback 0
2501A(config-if)#ip address 172.16.111.1 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#^z
2501A#copy run start
```

2. For router 2501B, configure the hostname, IP addresses, and loopback IP address (which will become the advertised BGP Router ID):

```
Router>enable
Router#config t
Router(config)#hostname 2501B
2501B(config)#int e0
2501B(config-if)#ip address 10.1.10.1 255.255.255.0
2501B(config-if)#no shut
2501B(config)#int loopback 0
2501B(config-if)#ip address 10.1.20.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#int s0
2501B(config-if)#ip address 172.16.11.2 255.255.255.0
2501B(config-if)#bandwidth 64
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
```

```
2501B(config-if)#^z
2501B#copy run start
```

3. Configure the 1900A switch with hostname and IP address, including the default gateway.

```
>enable
#config t
(config)#hostname 1900A
1900A(config)#ip address 172.16.15.2 255.255.255.0
1900A(config)#ip default-gateway 172.168.15.1
```

4. Configure the 1900B switch with hostname and IP address, including the default gateway.

```
>enable
#config t
(config)#hostname 1900B
1900B(config)#ip address 172.16.16.2 255.255.255.0
1900B(config)#ip default-gateway 172.16.16.1
```

Lab 8.2: Enabling BGP on Each Router

This lab shows how to configure two Cisco routers, which are identified by the hostname on each router, with BGP. This would probably never have real-world use but is a great example of how to configure a small BGP network between two autonomous systems.

1. Start BGP on 2501A. Identify the BGP neighbor and the neighbor's AS. Configure BGP to redistribute static routes and to advertise routes before a matching route is found by an IGP. Since this is the border router, configure a default route to the outside world.

When the remote-AS number of a neighbor is different from the router's own AS, this tells BGP that the neighbor is not part of the same network; eBGP will be used to peer with that neighbor.

```
2501A#config t
2501A(config)#router bgp 1
2501A(config-router)#network 172.16.0.0 mask
  255.255.255.0
2501A(config-router)#network 10.1.10.0 mask
  255.255.255.0
```

```
2501A(config-router)#network 10.1.20.0 mask
  255.255.255.0
2501A(config-router)#neighbor 172.16.11.2 remote-as 2
2501A(config-router)#redist static
2501A(config-router)#no synch
2501A(config)#ip route 0.0.0.0 0.0.0.0 s0
```

2. Start BGP on 2501B. Identify the BGP neighbor and the neighbor's AS. Configure BGP to redistribute static routes and to advertise routes before a matching route is found by an IGP, and configure a default route to 2501A.

```
2501B#config t
2501B(config)#router bgp 2
2501A(config-router)#network 172.16.0.0 mask
  255.255.255.0
2501B(config-router)#network 10.1.10.0 mask
  255.255.255.0
2501B(config-router)#network 10.1.20.0 mask
  255.255.255.0
2501B(config-router)#neighbor 172.16.11.1 remote-as 1
2501B(config-router)#redist static
2501B(config-router)#no synch
2501B(config)#ip route 0.0.0.0 0.0.0.0 s0
```

Lab 8.3: Verifying BGP Configurations

After BGP is configured, several commands will allow you to verify the BGP configuration and troubleshoot the operation of BGP. You can also use the same commands to monitor the BGP process and its operations.

Use the following commands to verify BGP on your routers:

Command	Description
`show ip bgp`	Shows all BGP configuration information for the selected interface.
`show ip bgp neighbors`	Shows all configured BGP neighbors. It provides detailed statistics and information about each neighbor.
`show ip bgp paths`	Displays all path information for the local router.
`show ip bgp summary`	Shows the status of all BGP connections.

Module 2: CCNP Switching Suggested Labs

These labs are designed to help you prepare for and pass the Cisco CCNP Switching exam (640-504). The labs follow the new Sybex *CCNP: Switching Study Guide*.

These labs can work in conjunction with any study guide or even as a stand-alone product. However, we recommend that you read the Sybex *CCNP: Switching Study Guide*, since all commands used in these labs are discussed and described in the book.

The following labs are covered in the Switching module and are based on topics discussed in detail in the *CCNP: Switching Study Guide*:

- Chapter 2: Connecting the Switch Block
- Chapter 3: VLANs
- Chapter 4: Layer 2 Switching and the Spanning Tree Protocol (STP)
- Chapter 5: Using Spanning Tree with VLANs
- Chapter 6: Inter-VLAN Routing

Labs from Chapter 2: Connecting the Switch Block

There are five labs for Chapter 2. These labs will have you set the hostname, banners, duplex, and interface descriptions on devices in the internetwork. You will then verify the configuration by pinging and telnetting into multiple devices. You will perform the following labs:

- Lab 2.1: Configuring the 1900A switch
- Lab 2.2: Configuring the 1900B switch
- Lab 2.3: Configuring the Catalyst 5000 series switch
- Lab 2.4: Configuring the 2621 router
- Lab 2.5: Verifying your configuration

Lab 2.1: Configuring the 1900A Switch

In this lab, you will log into a Cisco Catalyst 1900 switch and configure some basic command line interface (CLI) commands.

1. Configure the 1900A switch by going to the console and pressing k to enter the CLI.

   Type **k**

   You will receive the > prompt

2. Assign the user-mode password on 1900A. The 1900 switch uses the `level` command to set the user-mode and privileged-mode commands. Type the following commands to set the user-mode password:

   >enable

   #config t

   (config)#**enable password level 1 cisco**

3. Assign the enable password to the switch by using the **`level 15`** command.

   (config)#**enable password level 15 sanfran**

4. Assign the enable secret, which will override the enable password when set.

   (config)#**enable secret todd**

5. Set the hostname of the switch.

```
(config)#hostname 1900A
1900A(config)#
```

6. Set the IP address of the 1900A switch.

```
1900A(config)#ip address 172.16.1.3 255.255.255.0
```

7. Set the default gateway for the switch to the 2621 FastEthernet interface.

```
1900A(config)#ip default-gateway 172.16.1.1
```

8. Set interface f0/26 and f0/27 to run in full-duplex mode. By default they use auto-detect.

```
1900A(config)#int f0/26
1900A(config-if)#duplex full
1900A(config-if)#int f0/27
1900A(config-if)#duplex full
```

9. Set the descriptions of the two FastEthernet interfaces to Backbone Connection.

```
1900A(config-if)#int f0/26
1900A(config-if)#description backbone_connection
1900A(config-if)#int f0/27
1900A(config-if)#description backbone_connection
```

10. Type the command to view the current configuration.

```
1900A(config-if)#exit
1900A(config)#exit
1900A#show running-config
```

11. Verify the IP configuration of the switch.

```
1900A#show ip
```

12. Verify the configuration of interface FastEthernet f0/26.

```
1900A#show int f0/26
```

13. Configure interface e0/1 to full duplex and a description of VLAN 1.

```
1900A#config t
1900A(config)#int e0/1
1900A(config-if)#duplex full
1900A(config-if)#description pc_to_vlan1
```

14. Configure interface e0/2 to full duplex and a description of VLAN 2.

```
1900A(config-if)#int e0/2
1900A(config-if)#duplex full
1900A(config-if)#description pc_to_vlan2
```

15. Configure a banner on the switch.

```
1900A(config-if)#exit
```

```
1900A(config)#banner motd #
This is the 1900A switch
#
1900A(config)#
```

16. You do not need to perform a `copy run start` operation, because the switch automatically performs it. You can view the configuration by entering **`show running-config`**.

```
1900A(config)#exit
1900A#show running-config
```

Lab 2.2: Configuring the 1900B Switch

This lab will guide you through configuring the 1900B switch, which will then work in the internetwork designed for this product.

1. Configure the 1900B switch by going to the console and pressing k to enter the CLI.

```
Type k
You will receive the > prompt
```

2. Assign the user-mode password on 1900B. Type the following commands to set the user-mode password:

```
>enable
#config t
(config)#enable password level 1 cisco
```

3. Assign the enable password to the switch by using the **`level 15`** command.

```
(config)#enable password level 15 sanfran
```

4. Assign the enable secret, which will override the enable password when set.

```
(config)#enable secret todd
```

5. Set the hostname of the switch.

```
(config)#hostname 1900B
1900B(config)#
```

6. Set the IP address of the 1900B switch.

```
1900B(config)#ip address 172.16.1.4 255.255.255.0
```

7. Set the default gateway for the switch to the 2621 FastEthernet interface.

```
1900B(config)#ip default-gateway 172.16.1.1
```

8. Set interfaces f0/26 and f0/27 to run in full-duplex mode. By default they use auto-detect.

```
1900B(config)#int f0/26
1900B(config-if)#duplex full
1900B(config-if)#int f0/27
1900B(config-if)#duplex full
```

9. Set the descriptions of the two FastEthernet interfaces to Backbone Connection.

```
1900B(config-if)#int f0/26
1900B(config-if)#description backbone_connection
1900B(config-if)#int f0/27
1900B(config-if)#description backbone_connection
```

10. Type the command to view the current configuration.

```
1900B(config-if)#exit
1900B(config)#exit
1900B#show running-config
```

11. Verify the IP configuration of the switch.

```
1900B#show ip
```

12. Verify the configuration of interface FastEthernet f0/26.

```
1900B#show int f0/26
```

13. Configure interface e0/2 to full duplex and a description of VLAN3.

```
1900B#config t
1900B(config)#int e0/2
1900B(config-if)#duplex full
1900B(config-if)#description pc_on_vlan3
```

14. Configure a banner on the switch.

```
1900B(config-if)#exit
1900B(config)#banner motd #
This is the 1900B switch
#
1900B(config)#
```

15. You do not need to perform a `copy run start` operation, because the switch automatically performs it. You can view the configuration by entering **`show running-config`**.

```
1900B(config)#exit
1900B#show running-config
```

Lab 2.3: Configuring the Catalyst 5000 Series Switch

This lab will guide you through configuring the Catalyst 5000 series switch to work in the internetwork designed for this product.

1. When you first go to the 5000 series switch, you will be asked for a password before you can get to the user level and the privileged level. No password has been set up for either level, but you will still see a prompt for a password. Press Enter to go to the user mode and press Enter to go to the privileged level. Then set the prompt (hostname) to 5000A.

Once you set passwords for either level, you will have to enter the correct password in order to continue.

```
Enter password: [enter]
Console>en
Enter password: [enter]
Console>(enable) set prompt 5000A>
5000A>(enable)
```

2. Set the user-mode and enable passwords on the 5000 series switch. Enter any passwords that you want. If you are setting your passwords for the first time, just press Enter when it asks you to enter your old password. When you type the passwords, they do not appear on the screen. To set the user-mode password, use the command **set password**. To set the privileged password, use the command **set enablepass**.

```
5000A>(enable) set password
Enter old password: [enter]
Enter new password: <password>
Retype new password: <password>
Password changed.

5000A> (enable) set enablepass
Enter old password: [enter]
Enter new password: <password>
Retype new password: <password>
Password changed.
```

3. Set the IP address of the 5000A switch.

```
5000A> (enable) set int sc0 172.16.1.5 255.255.255.0
```

4. Type the command to see the configuration of the switch.

```
5000A> (enable) show config
```

5. Type the command to see the IP address of the switch.

```
5000A> (enable) show int
```

6. Configure the port speed and duplex of the connection to the 1900A switch.

```
5000A> (enable) set port speed 2/1 100
5000A> (enable) set port duplex 2/1 full
5000A> (enable) set port speed 2/2 100
5000A> (enable) set port duplex 2/2 full
```

7. Set the description of ports 2/1 and 2/2 to Link to 1900A.

```
5000A> (enable) set port name 2/1 link to 1900A
5000A> (enable) set port name 2/2 link to 1900A
```

8. Configure the port duplex of the connection to the 1900B switch. The speed cannot be changed on the supervisor card.

```
5000A> (enable) set port duplex 1/1 full
5000A> (enable) set port duplex 1/2 full
```

9. Set the descriptions of ports 2/1 and 2/2 to Link to 1900A.

```
5000A> (enable) set port name 1/1 link to 1900B
5000A> (enable) set port name 1/2 link to 1900B
```

10. Set the port speed to 100 and duplex to full on port 2/3, which is the connection to the 2621 router FastEthernet connection.

```
5000A> (enable) set port speed 2/3 100
5000A> (enable) set port duplex 2/3 full
```

11. Type the command to view port 1/1.

```
5000A> (enable) show port 1/1
```

12. Type the command to view the configuration of the 5000 switch.

```
5000A> (enable) show config
```

13. Ping from the 5000 switch console to both 1900 switches to test for connectivity.

```
5000A> (enable) ping 172.16.1.3
5000A> (enable) ping 172.16.1.4
```

14. Set a banner on the 5000 switch.

```
5000A> (enable) set banner motd #
This is the 5000A switch
#
banner set
```

Lab 2.4: Configuring the 2621 Router

This lab will provide you with the configuration necessary to have the 2600 router work with the internetwork designed with this product.

1. Press Enter to get a router prompt (>).
2. Type the command to enter privileged mode.

```
Router>ena
```

3. Type the command to enter configuration mode and change the running configuration.

```
Router>config t
```

4. Set the hostname to 2621.

```
Router(config)>hostname 2621
```

5. Set the banner on the 2621 router.

```
2621(config)>banner motd #
Enter TEXT message. End with the character '#'.
This is the 2621 router
#
```

6. Set the passwords on the 2621 router.

```
2621(config)>enable secret todd
2621(config)>line vty 0 4
2621(config-line)>login
2621(config-line)>password telnet
2621(config-line)>line con 0
2621(config-line)>login
2621(config-line)>password console
```

7. Go to interface FastEthernet 0/0 and set the IP address, description, speed, and duplex.

```
2621(config-line)>exit
2621(config)>int f0/0
2621(config-if)>ip address 172.16.1.1 255.255.255.0
2621(config-if)>description link to 5000A
2621(config-if)>full-duplex
2621(config-if)>speed 100
2621(config-if)>no shut
```

Lab 2.5: Verifying Your Configuration

After you have configured the switches, it is important to be able to verify your configuration. This lab will provide you with the commands necessary to verify your configuration.

1. From 1900A, ping all devices in the network. You cannot ping hosts that are not on the 172.16.1.0 network.

```
1900A#ping 172.16.1.1
1900A#ping 172.16.1.3
1900A#ping 172.16.1.4
1900A#ping 172.16.1.5
```

If you are not successful with all pings, troubleshoot the problem using Net Detective.

2. Type the commands used to see all active interface configurations.

```
1900A#show int f0/26
1900A#show int f0/27
1900A#show int e0/1
1900A#show int e0/2
```

3. From 1900B, ping all devices in the network.

```
1900B#ping 172.16.1.1
1900B#ping 172.16.1.2
1900B#ping 172.16.1.3
1900B#ping 172.16.1.5
```

4. Type the commands used to display all active interface configurations:

```
1900B#show int f0/26
1900B#show int f0/27
1900B#show int e0/1
1900B#show int e0/2
```

5. From the 5000A switch, ping all devices.

```
5000A> ping 172.16.1.1
5000A> ping 172.16.1.2
5000A> ping 172.16.1.3
5000A> ping 172.16.1.4
```

6. From the 5000A switch, telnet into all devices. You need to be in enable mode to telnet from a 5000 series switch.

You can only telnet into one device at a time. Type **exit** to go back to the 5000A switch.

```
5000A> ena
5000A>(enable) telnet 172.16.1.1
5000A>(enable) telnet 172.16.1.2
5000A>(enable) telnet 172.16.1.3
5000A>(enable) telnet 172.16.1.4
```

7. Type the commands to view the port configurations:

```
5000A>(enable) show config
5000A>(enable) show port 1/1
5000A>(enable) show port 1/2
5000A>(enable) show port 2/1
5000A>(enable) show port 2/2
5000A>(enable) show port 2/3
```

8. From the 2621 router, ping all devices.

```
2621#ping 172.16.1.2
2621#ping 172.16.1.3
2621#ping 172.16.1.4
2621#ping 172.16.1.5
```

9. From the 2621 router, telnet into other devices. To go back to the 2621 while in a telnet session, simultaneously press keys Ctrl+Shift+6, and then type x.

Type **show sessions** to see all open sessions.

```
2621#telnet 172.16.1.2
2621#telnet 172.16.1.3
2621#telnet 172.16.1.4
2621#telnet 172.16.1.5
```

10. All devices should be up and running and should be able to ping and telnet to each other. The 1900 switches can be telnetted into, but you cannot telnet from a 1900 switch console.
11. If you want to delete the configuration and perform the lab again, use the following commands:

    On the 1900 switches: **`delete nvram`**
    On the 5000A switch: **`clear config all`**
    On Router 2621: **`erase startup-config`** and **`reload`**

Labs from Chapter 3: VLANs

The labs in this section will have you configure the 5000 and 1900 switches with VTP and VLANs. You will perform these labs:

- Lab 3.1: Configuring VTP, trunking, and VLANs on the 5000 series switch
- Lab 3.2: Configuring VTP, trunking, and VLAN assignments on the 1900A switch
- Lab 3.3: Configuring VTP, trunking, and VLAN assignments on the 1900B switch

Lab 3.1: Configuring VTP, Trunking, and VLANs on the 5000 Series Switch

This lab will guide you through the configuration on the 5000 series switch, which will allow VTP and trunking to work in the internetwork.

1. Start with the 5000 series switch and configure the VTP domain as **`routersim`**.

   ```
   5000A>en
   5000A>(enable) set vtp domain routersim
   ```

2. The default VTP mode is server, which is what you want the 5000 series switch to be. The 1900 switches will be VTP clients. Create two new VLANs on the 5000 series switch.
   - VLAN 1 is the default; it will be used for management. The IP network is 172.16.1.0.
   - VLAN 2 will be the Sales VLAN and will use IP network 172.16.2.0.

- VLAN 3 will be the Mrkt VLAN and will use IP network 172.16.3.0.

Here is the configuration:

```
5000A>(enable) set vlan 2 name Sales
5000A>(enable) set vlan 3 name Mrkt
```

3. Type in the commands to verify the VLAN configuration and the VTP configuration.

```
5000A>(enable) show vtp
5000A>(enable) show vlan
```

4. Because you want VLAN information to be propagated to the 1900 switches, a trunked link needs to be configured between the two switches. Set the trunked link on ports 1/1 and 1/2 as well as 2/1 and 2/2 of the 5000 switch. These are your connections to the access layer switches (1900A and 1900B). Remember that the 1900 switch can use only ISL trunking, so the 5000 needs to be configured with ISL trunking.

```
5000A>(enable) set trunk 1/1 on isl
5000A>(enable) set trunk 1/2 on isl
5000A>(enable) set trunk 2/1 on isl
5000A>(enable) set trunk 2/2 on isl
```

5. Type the command to view the trunked link.

```
5000A>(enable) show trunk 1/1
5000A>(enable) show trunk 1/2
5000A>(enable) show trunk 2/1
5000A>(enable) show trunk 2/2
```

Lab 3.2: Configuring VTP, Trunking, and VLAN Assignments on the 1900A Switch

This lab will provide you with the steps to configure VTP and trunking on the 1900A switch.

1. Go to the 1900A switch and set the VTP domain name.

```
1900A#config t
1900A(config)#vtp domain routersim
```

2. Set the VTP mode to client.

```
1900A(config)#vtp client
```

3. Before any VLAN information will be propagated through the internetwork, you need to make both interfaces f0/26 and f0/27 a trunked link.

```
1900A(config)#int f0/27
1900A(config-if)#trunk on
1900A(config-if)#int f0/26
1900A(config-if)#trunk on
```

4. Verify that the trunked link is working.

```
1900A(config-if)#exit
1900A(config)#exit
1900A#show trunk a
1900A#show trunk b
```

5. Ping the 5000 series switch.

```
1900A#ping 172.16.1.5
```

6. Now verify that you have received VLAN information from the 5000 series switch.

```
1900A#show vlan
```

You should see all the configured VLANs.

7. Once you have the trunked link working and have received the VLAN information, you can assign VLANs to individual ports on the switch. Assign port 2 to VLAN 2.

```
1900A#config t
1900A(config)#int e0/2
1900A(config-if)#vlan-membership static 2
```

8. Verify the configuration.

```
1900A(config-if)#exit
1900A(config)#exit
1900A#show vlan-membership
1900A#show vlan
```

Lab 3.3: Configuring VTP, Trunking, and VLAN Assignments on the 1900B Switch

This lab will provide you with the steps to configure VTP and trunking on the 1900B switch.

1. Go to the 1900B switch and set the VTP domain name.

```
1900B#config t
1900B(config)#vtp domain routersim
```

2. Set the VTP mode to client.

```
1900B(config)#vtp client
```

3. Before any VLAN information will be propagated through the internetwork, you need to make both interfaces f0/26 and f0/27 a trunked link.

```
1900B(config)#int f0/27
1900B(config-if)#trunk on
1900B(config-if)#int f0/26
1900B(config-if)#trunk on
```

4. Verify that the trunked link is working.

```
1900B(config-if)#exit
1900B(config)#exit
1900B#show trunk a
1900B#show trunk b
```

5. Ping the 5000 series switch.

```
1900B#ping 172.16.1.5
```

6. Now verify that you have received VLAN information from the 5000 series switch.

```
1900B#show vlan
```

You should see all the configured VLANs.

7. Once you have the trunked link working and have received the VLAN information, you can assign VLANs to individual ports on the switch. Assign port 2 to VLAN 3.

```
1900B#config t
1900B(config)#int e0/2
1900B(config-if)#vlan-membership static 3
```

8. Verify the configuration.

```
1900B(config-if)#exit
1900B(config)#exit
1900B#show vlan-membership
1900B#show vlan
```

Labs from Chapter 4: Layer 2 Switching and the Spanning Tree Protocol (STP)

This section will teach you the basics of configuring the STP on Cisco catalyst switches. Here are the labs you will perform:

- Lab 4.1: Enabling and disabling Spanning Tree on the 5000 series switch
- Lab 4.2: Enabling and disabling Spanning Tree on the 1900 series switch

Lab 4.1: Enabling and Disabling Spanning Tree on the 5000 Series Switch

The first lab of this section will show you how to enable and disable STP on the 5000 series switch.

1. Type the command **show spantree** on the 5000 series switch.

   ```
   5000A>ena
   5000A >(enable) show spantree
   ```

2. By default, the **show spantree** command provides information only about VLAN 1. You can gather spanning-tree information about other VLANs by using the **show spantree *[vlan #]*** command.

   For example, to get information about VLAN 2, type the following command:

   ```
   5000A >(enable) show spantree 2
   ```

3. You can disable STP on all VLANs by using the following command:

   ```
   5000A>(enable) set spantree disable 1-1005
   Spantrees 1-1005 disabled.
   ```

4. Verify that STP is disabled by typing **show spantree** on the 5000 series switch.

   ```
   5000A >(enable) show spantree
   ```

5. You can enable STP on all VLANs by using the following command:

   ```
   5000A >(enable) set spantree enable 1-1005
   Spantrees 1-1005 enabled.
   ```

Lab 4.2: Disabling and Enabling Spanning Tree on the 1900 Series Switch

To enable or disable spanning tree on a Cisco IOS-based switch, use the **spantree** or **no spantree** command. The configuration below shows how to enable and disable spanning tree on a 1900 switch.

1. Use the **show spantree** command to see the STP information for VLAN 1. You can use the **show span** command for short.

```
1900A#show spantree
```

2. To disable spanning tree protocol for a VLAN, use the **no spantree** ***[vlan#]*** command. For example, to turn off spanning tree for VLAN 1, the command would be as follows:

```
1900A#config t
1900A(config)#no spantree 1
```

3. Verify that STP is disabled for VLAN 1.

```
1900A(config)#exit
1900A#sh span 1
Error: STP is not enabled for VLAN 1
```

4. To enable STP for a VLAN, enter the **spantree** ***[vlan#]*** command.

```
1900A#config t
1900A(config)#spantree ?
<1-1005>  ISL VLAN index
1900A(config)#spantree 1
```

5. Verify that the spanning tree protocol is running for VLAN 1.

```
1900A#sh span 1
VLAN1 is executing the IEEE compatible Spanning Tree Protocol
   Bridge Identifier has priority 32768, address 0030.80CC.7B40
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 32768, address 0030.80CC.7B40
   Root port is N/A, cost of root path is 0
   Topology change flag not set, detected flag not set
  Topology changes 0, last topology change occurred 0d00h00m00s ago
   Times:  hold 1, topology change 8960
           hello 2, max age 20, forward delay 15
   Timers: hello 2, topology change 35, notification 2
Port Ethernet 0/1 of VLAN1 is Forwarding
   [further output omitted]
```

Labs from Chapter 5: Using Spanning Tree with VLANs

To complete the labs for Chapter 5, you must have the configured both the 5000 series switch and the 1900 switch with the labs from Chapters 2 and 3. Each switch should have the hostname, interface descriptions, passwords, VTP domain information, and VLANs configured with trunked links on. You will perform the following labs:

- Lab 5.1: Enabling and testing PortFast on a switch
- Lab 5.2: Enabling UplinkFast on a switch
- Lab 5.3: Configuring the STP Root on the 5000 series switch
- Lab 5.4: Enabling EtherChannel between the 1900 and 5000 series switches

Lab 5.1: Enabling and Testing PortFast on a Switch

PortFast is disabled on all ports of a switch by default. By turning on PortFast, you can start forwarding up to 50 seconds sooner when bringing up a device. To test this, use HostA, which is plugged into interface e0/1 of the 1900A switch. You should never perform this on a switch port connected to another switch or hub.

1. From the DOS prompt of HostA, ping the 5000 series switch with the **-t** command.

   ```
   >ping -t 172.16.1.5
   ```

2. The **-t** will keep the ping running.

When you want to stop the pinging, click on the Host window and press Ctrl+C.

3. Go to the 1900A switch and perform **shutdown** and **no shutdown** commands on int e0/1; then notice how long it takes before the pings resume. This could be several seconds.

   ```
   1900A#config t
   1900A(config)#int e0/1
   ```

```
1900A(config-if)#shut
1900A(config-if)#no shut
```

4. Leave the pings running. Go to int e0/1 and type **spantree start-forwarding**, which turns on PortFast for that port.

```
1900A(config-if)#spantree start-forwarding
```

5. Go to the 1900A switch and perform another **shut** and then a **no shut** on e0/1. The pings will time out, but the time-out should resume after only a few seconds.

```
1900A(config-if)#shut
1900A(config-if)#no shut
```

Lab 5.2: Enabling UplinkFast on a Switch

This lab will provide you with the insight to enable UplinkFast on a Catalyst switch.

1. Leave the pings running, or restart the pinging from HostA to the 5000 series switch. Type **show spantree 1** and notice which port is forwarding and which port is blocking.

```
1900A#sh spantree 1
  Port FastEthernet 0/26 of VLAN1 is Blocking
  Port path cost 10, Port priority 128
  Designated root has priority 8192, address 00E0.3488.FC00
  Designated bridge has priority 8192, address 00E0.3488.FC00
  Designated port is 2, path cost 0
  Timers: message age 10, forward delay 7, hold 1

Port FastEthernet 0/27 of VLAN1 is Forwarding
  Port path cost 10, Port priority 128
  Designated root has priority 8192, address 00E0.3488.FC00
  Designated bridge has priority 8192, address 00E0.3488.FC00
  Designated port is 1, path cost 0
  Timers: message age 10, forward delay 7, hold 1
```

Notice that port f0/26 is in blocking mode and port f0/27 is in forwarding mode.

2. Leave pings running on HostA. Perform a **shutdown** on the forwarding interface. Notice that the pings have timed out, but they should resume after a few seconds, through interface f0/27.

```
1900A#config t
1900A(config)#int f0/26
1900A(config-if)#shut
```

3. Now type **show spantree 1** and notice which port is forwarding.

```
1900A#sh spantree 1
Port FastEthernet 0/26 of VLAN1 is Forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address 00E0.3488.FC00
   Designated bridge has priority 8192, address 00E0.3488.FC00
   Designated port is 2, path cost 0
   Timers: message age 10, forward delay 7, hold 1

Port FastEthernet 0/27 of VLAN1 is down
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address 00E0.3488.FC00
   Designated bridge has priority 8192, address 00E0.3488.FC00
   Designated port is 1, path cost 0
   Timers: message age 10, forward delay 7, hold 1
```

4. Perform a **no shutdown** on the interface you originally shut down. Notice that the pings have timed out again, but they should resume after a few seconds.

```
1900A#config t
1900A(config)#int f0/26
1900A(config-if)#no shut
```

5. Turn on UplinkFast on your 1900 forwarding port by typing **uplink-fast** from global configuration mode.

```
1900A(config-if)#exit
1900A(config)#exit
1900A(config)#uplink-fast
1900A(config)#exit
```

6. To verify that UplinkFast is configured and running, use the commands **show uplink-fast** and **show uplink-fast statistics**.

```
1900A#show uplink-fast
    Uplink fast                         Enabled
    Uplink fast frame generation rate   15
```

```
1900A#show uplink-fast statistics
    Uplink fast Transitions                 0
    Uplink fast Station Learning Frames     0
1900A#
```

7. Shut down the forwarding port again and notice that the ping time-out and resume cycle was shorter. UplinkFast will demonstrate an almost immediate transition to the second trunk link when the forwarding link has been shut down.

Lab 5.3: Configuring the STP Root on the 5000 Series Switch

This lab will provide you with the commands to set the 5000 series switch as an STP root bridge.

1. Configure the 5000 series switch as the STP root switch by typing **set spantree root 1-3 dia 2** from the enable mode of the switch. The diameter of the network is determined by counting the switches connected to the root, including the root, which in this case is 2. The VLANs configured are 1–3.

```
5000A> (enable) set spantree root ?
Usage: set spantree root [secondary] <vlans> [dia
<network_diameter>]
                              [hello <hello_time>]
     (vlans = 1..1005, network_diameter = 2..7, hello_time = 1..10)

5000A> (enable) set spantree root 1-3 dia 2
VLANs 1-2 bridge priority set to 8192.
VLANs 1-2 bridge max aging time set to 10.
VLANs 1-2 bridge hello time set to 2.
VLANs 1-2 bridge forward delay set to 7.
Switch is now the root switch for active VLANs 1-3.
5000A> (enable)
```

2. Verify the configuration by typing **show spantree 1**. Notice the root designation.

```
5000A> (enable) sh spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee
```

```
Designated Root              00-e0-34-88-fc-00
Designated Root Priority     8192
Designated Root Cost         0
Designated Root Port         1/0
Root Max Age   10 sec    Hello Time 2  sec   Forward Delay 7  sec

Bridge ID MAC ADDR           00-e0-34-88-fc-00
Bridge ID Priority           8192
Bridge Max Age 10 sec    Hello Time 2  sec   Forward Delay 7  sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start
--------- ----  -------------  -----  --------  ----------
 1/1      1     forwarding        19        32   disabled
 1/2      1     forwarding        19        32   disabled
 2/1      1     not-connected    100        32   disabled
 2/2      1     not-connected    100        32   disabled
 2/3      1     not-connected    100        32   disabled
 2/4      1     not-connected    100        32   disabled
 2/5      1     not-connected    100        32   disabled
--More-
```

Lab 5.4: Enabling EtherChannel Between the 1900 and 5000 Series Switches

Only the supervisor ports on the 5000 can run EtherChannel. You have to purchase an EtherChannel card to be able to run EtherChannel with more then the two ports on the supervisor module. Since 1900A is plugged into the two ports of the supervisor module (1/1-2), you can only set EtherChannel to 1900A.

1. Set the EtherChannel bundle to on for the 1900A switch by typing **port-channel mode on** from global configuration mode of the 1900A switch.

```
1900A(config)#port-channel mode ?
  auto          Set Fast EtherChannel mode to AUTO
  desirable     Set Fast EtherChannel mode to DESIRABLE
  off           Set Fast EtherChannel mode to OFF
  on            Set Fast EtherChannel mode to ON
1900A(config)#port-channel mode on
```

2. You must have the ports configured with trunking before EtherChannel can be enabled. To verify that the ports are trunking, use the **show trunk** command.

```
5000A> (enable) sh trunk
Port     Mode      Encapsulation  Status     Native vlan
-------- --------- -------------  ---------- -------
 1/1     on        isl            trunking      1
 1/2     on        isl            trunking      1
```

3. From the 5000 series switch, turn on EtherChannel by typing **set port channel 1/1-2 on**.

```
5000A> (enable) set port channel 1/1-2 on
Port(s) 1/1-2 channel mode set to on.
```

4. Verify the EtherChannel bundle by typing **show port channel**.

```
5000A> (enable) sh port channel
Port  Status  Channel Channel    Neighbor     Neighbor
      mode    status   device    port
-------------------------------------------------------
 1/1  connected  on    channel    cisco 1900  1900A    A
 1/2  connected  on    channel    cisco 1900  1900A    B
-------------------------------------------------------
```

Labs from Chapter 6: Inter-VLAN Routing

This section will show you how to configure Inter-VLAN configuration on both an internal processor and external route processor. Here are the labs you will perform:

- Lab 6.1: Using the 2621 router to perform ISL routing
- Lab 6.2: Configuring the RSM in the 5000 Switch for inter-VLAN Routing Using ISL

Lab 6.1: Using the 2621 Router to Perform ISL Routing

The 2621 router will provide the inter-VLAN routing and allow the hosts to communicate with each other.

1. Go to the privileged mode of Router 2621 and enter into the global configuration mode.

```
Router> ena
Router#config t
Router(config)#
```

2. Configure the FastEthernet interface to run ISL routing for all three VLANs. You first need to remove the IP address from interface f0/0 on the 2621.

```
2621(config)#int f0/0
2621(config-if)#no ip address
2621(config-if)#int f0/0.1
2621(config-subif)#encap isl 1
2621(config-subif)#ip address 172.16.1.1 255.255.255.0
2621(config-subif)#int f0/0.2
2621(config-subif)#encap isl 2
2621(config-subif)#ip address 172.16.2.1 255.255.255.0
2621(config-subif)#int f0/0.3
2621(config-subif)#encap isl 3
2621(config-subif)#ip address 172.16.3.1 255.255.255.0
2621(config-subif)#int f0/0
2621(config-if)#no shut
2621(config-if)#
```

3. Before this will work, you need to set the port on the 5000 to trunk mode. Go to the 5000 switch and configure the port to trunk.

```
5000A> (enable) set trunk 2/3 on
Port(s) 2/3 trunk mode set to on.
```

4. Verify that the ISL routing is working by pinging between hosts.

Lab 6.2: Configuring the RSM in the 5000 Switch for inter-VLAN Routing Using ISL

The 2621 router will not be needed in this lab, and you should shut down the f0/0 interface to stop it from routing.

1. Shut down the 2621 router interface to the 5000 series switch. The hosts can no longer be able ping each other.

```
2621(config)#int f0/0
2621(config-if)#shut
```

2. Configure the RSM on the 5000 series switch to provide inter-VLAN routing. Use the **show module** command to view the RSM card location.

```
5000A> (enable) sh module
Mod Module-Name  Ports Module-Type Model Serial-Num Status
---------------------------------------------------------
1    2   100BaseTX Supervisor    WS-X5509    005147178  ok
2    12  10/100BaseTX Ethernet   WS-X5213A   005153813  ok
4        Route Switch Ext Port
5    1   Route Switch            WS-X5304    018465234  ok
```

3. Notice that the RSM in is module 5. Connect to the RSM through the 5000 console by using the **session** command.

```
5000A> (enable) session 5
Trying Router-5...
Connected to Router-5.
Escape character is '^]'.
Router>
```

4. Configure three VLAN interfaces, one for each VLAN configured in the switched internetwork. Notice that the same IP addresses are used, so the host's default gateway does not have to be reconfigured.

```
Router> en
Router#config t
Enter configuration commands, one per line.  End with
  CNTL/Z.
Router(config)#hostname 5000RSM
5000RSM(config)#int vlan 1
5000RSM(config-if)#ip address 172.16.1.1 255.255.255.0
5000RSM(config-if)#no shut
```

```
5000RSM(config-if)#int vlan 2
5000RSM(config-if)#ip address 172.16.2.1 255.255.255.0
5000RSM(config-if)#no shut
5000RSM(config-if)#int vlan 3
5000RSM(config-if)#ip address 172.16.3.1 255.255.255.0
5000RSM(config-if)#no shut
```

5. Verify that the RSM is working by pinging between hosts.

Module 3: Remote Access Suggested Labs

These labs are designed to help you prepare for and pass the Cisco CCNP Remote Access exam (640-505). The labs follow the Sybex *CCNP: Remote Access Study Guide*, written by industry experts Robert Padjen and Todd Lammle, with Sean Odom.

These labs can work in conjunction with any study guide or even as a stand-alone product. However, we recommend that you read the Sybex *CCNP: Remote Access Study Guide* since all commands used in these labs are discussed and described in the book.

The following labs are covered in the Remote Access module and are based on topics discussed in detail in the *CCNP: Remote Access Study Guide*:

- Chapter 3: Point-to-Point Protocol
- Chapter 5: Integrated Services Digital Network (ISDN)
- Chapter 6: Cisco 700 Series
- Chapter 7: X.25 and LAPB
- Chapter 8: Frame Relay

Labs from Chapter 3: Point-to-Point Protocol

The labs in this section correspond directly with Chapter 3 of the Sybex *CCNP: Remote Access Study Guide*. They show how to configure Cisco routers with the Point-to-Point Protocol and use CHAP authentication between serial links.

We recommend setting the passwords on each router for practice, but that is not required in these labs. To begin these labs, you need to delete any existing configurations from all routers and switches. You then will configure the three 2500 routers with the PPP encapsulation. We will be using the 172.16.0.0/24 network address and assigning the IP addresses as shown in the Network Visualizer.

This section includes the following lab exercises:

- Lab 3.1: Deleting the router configurations
- Lab 3.2: Assigning IP addresses to the routers
- Lab 3.3: Enabling EIGRP on the routers
- Lab 3.4: PPP configuration
- Lab 3.5: PPP authentication
- Lab 3.6: Verifying the PPP configuration

Lab 3.1: Deleting the Router Configurations

If you have previously configured the routers before attempting this module, make sure that you delete the configuration on your routers. Use the following information from if necessary.

1. Go to the 2501A router and type erase startup-config; then reload the router.

```
2501A>ena
2501A#erase startup-config
2501A#reload
```

2. Go to the 2501B router and type erase startup-config; then reload the router.

```
2501B>ena
2501B#erase startup-config
2501B#reload
```

3. Go to the 2501C router and type erase **startup-config;** then reload the router.

```
2501C>ena
2501C#erase startup-config
2501C#reload
```

Lab 3.2: Assigning IP Addresses to the Routers

In this section, you will configure the basic configuration on your routers.

1. Configure the hostname, IP addresses, and enable password for the 2501A router.

```
Router>enable
Router#config t
Router(config)#enable password cisco
Router(config)#hostname 2501A
2501A(config)#interface s0
2501A(config-if)#ip address 172.16.20.1 255.255.255.0
2501A(config-if)#bandwidth 64
2501A(config-if)#no shutdown
2501A(config-if)#interface e0
2501A(config-if)#ip address 172.16.10.1 255.255.255.0
2501A(config-if)#no shutdown
2501A(config-if)#^z
2501A#copy run start
```

2. Configure the hostname, IP addresses, and enable password for the 2501B router.

```
Router>enable
Router#config t
Router(config)#enable password cisco
Router(config)#hostname 2501B
2501B(config)#interface s0
2501B(config-if)#ip address 172.16.40.1 255.255.255.0
2501B(config-if)#bandwidth 64
2501B(config-if)#no shut
2501B(config-if)#interface e0
2501B(config-if)#ip address 172.16.50.1 255.255.255.0
2501B(config-if)#no shut
```

```
2501B(config-if)#^z
2501B#copy run start
```

3. Configure the hostname, IP addresses, and enable password for the 2501C router. The 2501C has DCE connection on both serial links, so you need to add the `clock rate` command to each serial interface configuration.

```
Router>enable
Router#config t
Router(config)#enable password cisco
Router(config)#hostname 2501C
2501C(config)#interface e0
2501C(config-if)#ip address 172.16.30.1 255.255.255.0
2501C(config-if)#no shut
2501C(config)#interface s0
2501C(config-if)#ip address 172.16.20.2 255.255.255.0
2501C(config-if)#bandwidth 64
2501C(config-if)#clock rate 64000
2501C(config-if)#no shut
2501C(config-if)#int s1
2501C(config-if)#ip address 172.16.40.2 255.255.255.0
2501C(config-if)#bandwidth 64
2501C(config-if)#clock rate 64000
2501C(config-if)#no shut
2501C(config-if)#^z
2501C#copy run start
```

Lab 3.3: Enabling EIGRP on the Routers

To have all routers share connected network information, you need to add a routing protocol. This lab will have you turn on EIGRP.

1. Start EIGRP on 2501A, and then identify the AS number and the directly connected classful networks.

```
2501A#config t
2501A(config)#router eigrp 10
2501A(config-router)#network 172.16.0.0
```

2. Start EIGRP on 2501B, and then identify the AS number and the directly connected networks.

```
2501B#config t
2501B(config)#router eigrp 10
2501B(config-router)#network 172.16.0.0
```

3. Start EIGRP on 2501C, and then identify the AS number and the directly connected networks.

```
2501C#config t
2501C(config)#router eigrp 10
2501C(config-router)#network 172.16.0.0
```

At this point you should be able to ping all the router interfaces. You can also use the `show ip interface brief` command to see the active interfaces and the `show ip route` command to see all the known routes.

Lab 3.4: PPP Configuration

By default, Cisco routers use High-level Data Link Control (HDLC) as a point-to-point encapsulation method on serial links. If you are connecting to non-Cisco equipment or wish to have a more secure connection, you can enable the use of PPP encapsulation.

1. On the 2501A router, configure the Serial 0 interface connecting to 2501C to use PPP encapsulation instead of HDLC.

```
2501A(config)#interface s0
2501A(config-if)#encap ppp
```

2. On the 2501C router, configure the Serial 0 interface connecting to 2501A and the Serial 1 interface connecting to 2501B to use PPP encapsulation instead of HDLC.

```
2501C(config)#interface s0
2501C(config-if)#encap ppp
2501C(config-if)#interface s1
2501C(config-if)#encap ppp
```

3. On the 2501B router, configure the Serial 0 interface connecting to 2501C to use PPP encapsulation instead of HDLC.

```
2501B(config)#interface s0
2501B(config-if)#encap ppp
```

Lab 3.5: PPP Authentication

Follow these steps to enable PPP on your serial links and create a username and password on each device. Because we have configured an enable password on each device, the hostname of the device is the username, and the enable password is the password we will use for authentication (although

it doesn't have to be the same as the enable secret password). The passwords just need to be the same on both routers.

1. On the 2501A router, configure the username and password needed to authenticate to 2501C; then configure PPP to use CHAP authentication.

```
2501A(config)#username 2501C password cisco
2501A(config)#interface s0
2501A(config-if)#ppp authentication chap
```

2. On the 2501C router, configure the Serial 0 interface connecting to 2501A and the Serial 1 interface connecting to 2501B to use PPP CHAP authentication and configure the username and password needed to authenticate to 2501A and 2501C.

```
2501C(config)#username 2501A password cisco
2501C(config)#username 2501B password cisco
2501C(config)#interface s0
2501C(config-if)#ppp authentication chap
2501C(config-if)#interface s1
2501C(config-if)#ppp authentication chap
```

3. On the 2501B router, configure PPP to use CHAP authentication and configure the username and password needed to authenticate to 2501C.

```
2501B(config)#username 2501C password cisco
2501B(config)#interface s0
2501B(config-if)#ppp authentication chap
```

Lab 3.6: Verifying the PPP Configuration

To verify the configuration, use the `show ip route` and `show interface` commands on each router.

1. First verify that all routes are in the routing tables of each router by using the `show ip route` command. If the routes are not present, check your username and authentication for PPP on the serial links. The username and passwords are case sensitive, and the passwords must also be the same on both routers.

```
2501A#sh ip route

2501B#sh ip route

2501C#sh ip route
```

2. Use the `show interface` command to verify the PPP configuration on the serial links. Make sure that LCP is open and the IPCP and CDPCP are showing in the output. This is IP and CDP within the NCP header of PPP. See the Sybex *CCNP: Remote Access Study Guide*, Chapter 3, for detailed information about NCP.

```
2501A#sh int s0

2501B#sh int s0

2501C#sh int s0
```

Labs from Chapter 5: Integrated Services Digital Network (ISDN)

The labs in this section correspond directly with Chapter 5 of the Sybex *CCNP: Remote Access Study Guide*. The purpose of this series of labs is to configure ISDN between two Cisco 804 routers. You will have successfully completed these labs when the routers dial up ISDN automatically after interesting traffic is found. To begin these labs, you will delete any existing configurations from the 804 routers.

This section includes the following lab exercises:

- Lab 5.1: Deleting the router configurations
- Lab 5.2: Assigning hostnames and ISDN switch-types to the routers
- Lab 5.3: Setting the service provider ID (SPID) and IP addresses
- Lab 5.4: Creating the routes
- Lab 5.5: Specifying interesting traffic to bring up the link
- Lab 5.6: Configuring the dialer information
- Lab 5.7: Verifying the ISDN connection

Here are the lab IP addresses we will use in the labs:

```
804A
BRI0: 172.16.60.1/24
E0: 172.16.10.1/24
804B
BRI0: 172.16.60.2/24
E0: 172.16.20.1/24
```

Lab 5.1: Deleting the Router Configurations

In this lab, if you had previously set up the routers, you will delete any possible configuration on the 804 routers. If you have not configured the routers previously, skip ahead to lab 5.2.

1. Go to the 804A router and type erase startup-config; then reload the router.

```
804A>ena
804A#erase startup-config
804A#reload
```

2. Go to the 804B router and type erase startup-config; then reload the router.

```
804B>ena
804B#erase startup-config
804B#reload
```

Lab 5.2: Assigning Hostnames and ISDN Switch-Types to the Routers

In this lab, you will set the hostname of the routers and the ISDN provider's switch-type. Before you take your Remote Access exam, it's important to understand that you can set the switch-type either from global configuration mode or from interface configuration. For that reason, this lab demonstrates both techniques, setting the switch-type for the first router at the global configuration level and for the second router at the interface level (even though there is no technical reason at this point to configure the switch-type at interface level). The ISDN switch used is configured with a default ISDN switch-type of `basic-ni`.

1. Go to the 804A router and set the hostname and ISDN switch type.

```
Router#config t
Router(config)#hostname 804A
804A(config)#isdn switch-type basic-ni
```

2. Set the hostname and switch type on 804B at the interface level.

```
Router#config t
Router(config)#hostname 804B
804B(config)#int bri0
804B(config-if)#isdn switch-type basic-ni
```

Lab 5.3: Setting the Service Provider ID (SPID) and IP Addresses

In this lab, you will set the SPID numbers under the BRI interface of each router. The Service Provider IDs (SPIDs) are used to identify your B (bearer) channels. Basic Rate Interface (BRI) uses two B channels, so two SPID numbers are used for each BRI interface.

The following SPIDs are configured on the ISDN switch. (If you do not match these numbers exactly, the link will not come up.)

804A SPIDs:

```
0835866101 8358661
0835866301 8358663
```

804B SPIDs:

```
0835866201 8358662
0835866401 8358664
```

To set the SPIDs on an interface, use the `isdn spid1` and `isdn spid2` commands. Notice that there is no space between `spid` and the number of the B channel (1 or 2). The second set of numbers used in the command is used for administration purposes only, as it displays the phone number of the B channel. This is optional and not required in ISDN.

1. On 804A, set the SPID numbers on the BRI 0 interface and set the IP addresses.

```
804A#config t
804A(config)#int bri0
804A(config-if)#isdn spid1 0835866101 8358661
804A(config-if)#isdn spid2 0835866301 8358663
804A(config-if)#ip address 172.16.60.1 255.255.255.0
804A(config-if)#no shut
804A(config-if)#int e0
804A(config-if)#ip address 172.16.10.1 255.255.255.0
804A(config-if)#no shut
804A(config-if)#exit
804A(config)#exit
804A#copy running-config startup-config
```

As a shorthand alternative, you can enter the last command above as simply `copy run start`. We will use the shorthand form throughout this module.

2. On 804B, set the SPID numbers BRI 0 interface and set the IP addresses.

```
804B#config t
804B(config)#int bri0
804B(config-if)#isdn spid1 0835866201 8358662
804B(config-if)#isdn spid2 0835866401 8358664
804B(config-if)#ip address 172.16.60.2 255.255.255.0
804B(config-if)#no shut
804B(config-if)#int e0
804B(config-if)#ip address 172.16.20.1 255.255.255.0
804B(config-if)#no shut
804B(config-if)#exit
804B(config)#exit
804B#copy run start
```

Lab 5.4: Creating the Routes

Create static routes on the routers to use the remote ISDN interface. Static routes, instead of dynamic routing, are recommended with ISDN DDR so that the link is not brought up by route updates.

1. Configure the 804A with a static IP route to network 172.16.20.0/24. You need two configuration lines: one to tell the router how to get to network 172.16.20.0, which is 172.16.60.2, and the second to describe how to get to 172.16.60.2.

```
804A(config)#ip route 172.16.20.0 255.255.255.0
   172.16.60.2
804A(config)#ip route 172.16.60.2 255.255.255.255 bri0
```

2. Configure the 804B with a static IP route to network 172.16.10.0/24. You need two configuration lines: one to tell the router how to get to network 172.16.0.0, which is 172.16.60.1, and the second to describe how to get to 172.16.60.1.

```
804B(config)#ip route 172.16.10.0 255.255.255.0
   172.16.60.1
804B(config)#ip route 172.16.60.1 255.255.255.255 bri0
```

Lab 5.5: Specifying Interesting Traffic to Bring Up the Link

This lab will have you choose and permit all IP traffic and then apply it to the BRI interface of both routers.

1. Specify interesting traffic to bring up the ISDN link. This is a global configuration mode command: `dialer-list access-list number protocol protocol deny/permit`.

```
804A(config)#dialer-list 1 protocol ip permit

804B(config)#dialer-list 1 protocol ip permit
```

2. Under the BRI interface of both routers, add the command `dialer-group 1`, which matches the dialer-list number. This tells the router to go to BRI0 when IP traffic is found.

```
804A(config)#config t
804A(config)#int bri0
804A(config-if)#dialer-group 1

804B(config)#config t
804B(config)#int bri0
804B(config-if)#dialer-group 1
```

Lab 5.6: Configuring the Dialer Information

This lab will have you configure the dial number used by the BRI interface of each router. Optional commands will also be set on each interface.

1. Configure the dialer information on both routers. This tells the BRI interface which number to dial when interesting traffic is found.

```
804A#config t
804A(config)#int bri0
804A(config-if)#dialer string 8358662

804B#config t
804B(config)#int bri0
804B(config-if)#Dialer string 8358661
```

2. Set the `dialer load-threshold` and `multilink` command, as well as the idle time percentage on both 804 routers.

```
804A#config t
804A(config)#int bri0
804B(config-if)#dialer load-threshold 125 either
804B(config-if)#dialer idle-timeout 180

804B#config t
804B(config)#int bri0
804B(config-if)#dialer load-threshold 125 either
804B(config-if)#dialer idle-timeout 180
```

The above commands set the BRI interfaces to bring up the second B channel when the first B channel is at 50% capacity from either inbound or outbound traffic. Also, the `dialer idle-timeout` command tells the router to drop BRI0 when no interesting traffic is found for 180 seconds.

3. Set the hold queue for packets when they are found interesting and need a place to wait for the ISDN link to come up so they are not dropped.

```
804A#config t
804A(config)#int bri0
804B(config-if)#hold-queue 75 in

804B#config t
804B(config)#int bri0
804B(config-if)#hold-queue 75 in
```

Lab 5.7: Verifying the ISDN Connection

It is very important that you can verify your configuration and that ISDN is working. This lab will provide you with verification commands you can use to check ISDN on Cisco routers.

1. From the 804A router command-line interface, ping to the IP address 172.16.20.1. This will bring up the ISDN line. The first two pings will be a time-out because of the time it takes for the interface BRI0 to come up. After the link is up, you should be able to ping to the IP addresses configured on the 804B router.
2. From the 804B router, ping the IP address 172.16.10.1.

```
804B#ping 172.16.10.1
```

3. If you set the VTY passwords on your routers, you should also be able to Telnet from one router to the other. Here is a reminder on how to set the password for telnet access:

```
804A#config t
804A(config)#line vty 0 4
804A(config-line)#login
804A(config-line)#password cisco
```

You should now be able to telnet into the 804A router from the console of the 804B router.

4. Use the `show dialer` command on both routers to see the ISDN dialer information.

```
804A#show dialer

804B#show dialer
```

Labs from Chapter 6: Cisco 700 Series

The labs in this section correspond directly with Chapter 6 of the Sybex *CCNP: Remote Access Study Guide*. The Cisco 700 series routers and their configuration commands can be confusing, so be sure to read the chapter before attempting these labs.

In this series of labs you will configure two Cisco 700 series routers to connect two Ethernet LAN segments across an ISDN link using the Combinet command-line interface, which is similar to the Crescendo (Set/Clear) command-line interface. To begin these labs, make sure you delete the configurations from the 700 series routers if you have previously used them.

This section includes the following lab exercises:

- Lab 6.1: Deleting the router configurations
- Lab 6.2: Configuring the 700A router
- Lab 6.3: Configuring the 700B router
- Lab 6.4: Activating the BRI interface

Lab 6.1: Deleting the Router Configurations

In this lab, you will delete any existing configuration on your routers. If you have not configured the routers previously, skip ahead to lab 6.2.

1. Go to the 700A router and type set default.

   ```
   700A>set default
   ```

2. Go to the 700B router and type set default.

   ```
   700B>set default
   ```

Lab 6.2: Configuring the 700A Router

In this lab, you will configure the basic configuration on the 700A router. We are using a Cisco 776M router with four Ethernet interfaces and an ISDN S/T interface. We will be configuring the 700A router with information found in the following table for the Ethernet and BRI (ISDN U) interfaces:

Parameter	Value
Ethernet IP address	172.16.10.1/24
BRI0 IP address	172.16.60.1/24
Protocol	IP
Hostname	700A
Bridging	Off
IP routing	On
Encapsulation	PPP
ISDN Switch Type	NI1
SPID 1 (if one is not assigned on the simulator)	0835866101
SPID 2 (if one is not assigned on the simulator)	0835866301
RIP version	1
Remote Profile name	700B
Remote dial number	8358662

1. First we will configure the configuration necessary on the global interface. Set the hostname, the date, switch type, SPID 1, SPID 2, and RIP version 1.

```
Router>set systemname 700A
700A>set switch nil
700A>set date 9/11/2001
700A>set 1 spid 0835866101
700A>set 2 spid 0835866301
700A>set ip rip version 1
700A>set ip routing on
```

2. Next configure the ports connected to the local LAN. Configure the IP address and subnet mask, and enable periodic routing updates.

```
700A>cd lan
700A:LAN>set ip address 172.16.10.1
700A:LAN>set ip netmask 255.255.255.0
700A:LAN>set ip routing on
700A:LAN>set ip rip update periodic
```

3. Configure the remote connection settings for the ISDN BRI interface. Configure the interface's IP address and subnet mask, enable RIP version 1 and PPP encapsulation, and turn bridging off.

```
700A:LAN>cd
700A >set user 700B
700A:700B>set ip address 172.16.20.1
700A:700B>set ip netmask 255.255.255.0
700A:700B>set ip routing on
700A:700B>set ip rip update periodic
700A:700B>set ip rip version 1
700A:700B>set encapsulation ppp
700A:700B>set number 8358662
700A:700B>set bridging off
```

Lab 6.3: Configuring the 700B Router

In this section, you will configure the basic configuration on the 700B router. We will be configuring the 700B router with information found in the following table for the Ethernet and BRI (ISDN U) interfaces:

Parameter	Value
Ethernet IP address	172.16.20.1/24
BRI0 IP address	172.16.60.2/24

Parameter	Value
Protocol	IP
Hostname	700B
Bridging	Off
IP routing	On
Encapsulation	PPP
ISDN Switch Type	NI1
SPID 1 (if one is not assigned on the simulator)	0835866201
SPID 2 (if one is not assigned on the simulator)	0835866401
RIP version	1
Remote Profile name	700A
Remote dial number	8358661

1. Configure the configuration necessary on the global interface for the 700B router. Set the hostname, the date, switch type, SPID 1, SPID 2, and RIP version 1.

```
Router>set systemname 700B
700B>set switch ni1
700B>set date 9/11/2001
700B>set 1 spid 0835866201
700B>set 2 spid 0835866401
700B>set ip rip version 1
700B>set ip routing on
```

2. Next configure the ports connected to the local LAN and the 700B switch. Configure the IP address and subnet mask, and enable periodic routing updates.

```
700B>cd lan
700B:LAN>set ip address 172.16.20.1
700B:LAN>set ip netmask 255.255.255.0
700B:LAN>set ip routing on
700B:LAN>set ip rip update periodic
```

3. Configure the remote connection settings for the ISDN BRI interface. Configure the interface's IP address and subnet mask, enable RIP version 1 over the connection, enable PPP encapsulation, and turn bridging off.

```
700B:LAN>cd
700B>set user 700A
700B:700A>set ip address 172.16.10.1
700B:700A>set ip netmask 255.255.255.0
700B:700A>set ip routing on
700B:700A>set ip rip update periodic
700B:700A>set ip rip version 1
700B:700A>set encapsulation ppp
700B:700A>set number 8358661
700B:700A>set bridging off
```

Lab 6.4: Activating the BRI Interface

This lab will have you bring up the BRI interfaces on the two 700 series routers.

1. On the 700B router make the interface active, forcing the router to bring up the BRI channel to the 700A router; then ping the IP address on the 700A router BRI.

```
700B:700A>set active 700A

700B>CCBRI_Go: ces: 1 call_id: 7 call_ref: 89
      01/11/2001 00:04:14  L18  1   Terminal Identifier Assigned
700B> 01/11/2001 00:04:14  L22  1   0835866201  Sending SPID
700B> 01/11/2001 00:04:14  L18  2   Terminal Identifier Assigned
700B> 01/11/2001 00:04:14  L23  1   0835866201  SPID Accepted
700B> 01/11/2001 00:04:14  L22  2   0835866401  Sending SPID
700B> 01/11/2001 00:04:14  L23  2   0835866401  SPID Accepted
700B> 01/11/2001 00:04:25  L11  1   8358661  Call Requested
700B> 01/11/2001 00:04:25  L14  1    Accepting Call
700B> CCBRI_Go: ces: 1 call_id: 8 call_ref: 8b
01/11/2001 00:04:26  L08  1      8358661  Call Connected
700B> 01/11/2001 00:04:29  Connection 2 Add     Link 1 Channel 1

700B> ping 172.16.10.2
Start sending:   round trip time is 50 msec.

700B>
```

2. You can use the `show config` command to view the configuration of the router.

Labs from Chapter 7: X.25 and LAPB

The labs in this section correspond directly with Chapter 7 of the Sybex *CCNP: Remote Access Study Guide*. In these labs you will configure an X.25 encapsulated link using LABP at layer 2 and IP address along with the X.121 address. You will configure X.25 between the 2501A router and the 2501B router. You will then configure a standard HDLC serial connection between routers 2501B and 2501C.

To begin these labs, delete any existing configurations from all routers. This section includes the following lab exercises:

- Lab 7.1: Deleting the router configurations
- Lab 7.2: Assigning IP addresses to the routers
- Lab 7.3: Configuring X.25
- Lab 7.4: Configuring EIGRP
- Lab 7.5: Verifying X.25

Lab 7.1: Deleting the Router Configurations

In this lab, you will delete the configuration on your routers.

1. Go to the 2501A router and type erase startup-config; then reload the router.

```
2501A>ena
2501A#erase startup-config
2501A#reload
```

2. Go to the 2501B router and type erase startup-config; then reload the router.

```
2501B>ena
2501B#erase startup-config
2501B#reload
```

3. Go to the 2501C router and type erase startup-config; then reload the router.

```
2501C>ena
2501C#erase startup-config
2501C#reload
```

Lab 7.2: Assigning IP Addresses to the Routers

This lab will have you configure the 2500 routers and prepare the routers to run X.25 as a serial encapsulation.

1. Configure the hostname and IP addresses that will be advertised by EIGRP when X.25 is configured correctly on the 2501A router.

```
Router>enable
Router#config t
Router(config)#hostname 2501A
2501A(config)#interface s0
2501A(config-if)#ip address 172.16.10.1 255.255.255.0
2501A(config-if)#no shutdown
2501A(config-if)#interface s0
2501A(config-if)#ip address 172.16.20.1 255.255.255.0
2501A(config-if)#no shutdown
2501A(config-if)#^z
2501A#copy run start
```

2. Configure the hostname and IP addresses that will be advertised by EIGRP when X.25 is configured correctly on the 2501B router.

```
Router>enable
Router#config t
Router(config)#hostname 2501B
2501B(config)#interface e0
2501B(config-if)#ip address 172.16.50.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#interface s0
2501B(config-if)#ip address 172.16.40.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#^z
2501B#copy run start
```

3. Configure the hostname, IP addresses, and clock rates that will be used on the 2501C router.

```
Router>enable
Router#config t
Router(config)#hostname 2501C
2501C(config)#interface e0
2501C(config-if)#ip address 172.16.30.1 255.255.255.0
2501C(config-if)#no shut
```

```
2501C(config-if)#int s0
2501C(config-if)#ip address 10.1.20.2 255.255.255.0
2501C(config-if)#clock rate 64000
2501C(config-if)#no shut
2501C(config-if)#int s1
2501C(config-if)#ip address 172.16.40.2 255.255.255.0
2501C(config-if)#clock rate 64000
2501C(config-if)#no shut
2501C(config-if)#^z
2501C#copy run start
```

Lab 7.3: Configuring X.25

This lab will have you change the serial encapsulation to X.25. After you are done configuring the routers, the interface should come up. If it does not, shut down the interface and restart it using the **shutdown** command and then **no shutdown**.

Use the following X.25 addresses:

```
2501A S0: 3129165551212
2501B S0: 3129165551312
2501C S0: 3129165551211
2501C S1: 3129165551311
```

1. Configure X.25 and the X.121 address, and map the IP address of the opposite side of the link on the 2501A router.

```
2501A#config t
2501A(config)#int s0
2501A(config-if)#encapsulation x25 dce
2501A(config-if)#x25 address 3129165551212
2501A(config-if)#x25 ltc 10
2501A(config-if)#x25 htc 100
2501A(config-if)#x25 map ip 172.16.20.2 3129165551211
  broadcast
2501A(config-if)#no shut
```

2. Configure X.25 and the X.121 address, and map the IP address of the opposite side of the link on the 2501C router.

```
2501C#config t
2501C(config)#int s0
2501C(config-if)#encapsulation x25 dte
2501C(config-if)#x25 address 3129165551211
```

```
2501C(config-if)#x25 ltc 10
2501C(config-if)#x25 htc 100
2501C(config-if)#x25 map ip 172.16.20.1 3129165551212
  broadcast
2501C(config-if)#no shut
2501C(config-if)#int s1
2501C(config-if)#encapsulation x25 dce
2501C(config-if)#x25 address 3129165551311
2501C(config-if)#x25 ltc 10
2501C(config-if)#x25 htc 100
2501C(config-if)#x25 map ip 172.16.40.1 3129165551312
  broadcast
2501C(config-if)#no shut
```

3. Configure X.25 and the X.121 address, and map the IP address of the opposite side of the link on the 2501B router.

```
2501B(config-if)#int s0
2501B(config-if)#encapsulation x25 dte
2501B(config-if)#x25 address 3129165551312
2501B(config-if)#x25 ltc 10
2501B(config-if)#x25 htc 100
2501B(config-if)#x25 map ip 172.16.40.2 3129165551311
  broadcast
2501B(config-if)#no shut
```

Lab 7.4: Configuring EIGRP

To have all routers share connected network information, you need to add a routing protocol. This lab will have you turn on EIGRP.

1. Start EIGRP on 2501A, and identify the AS number and the directly connected classful networks.

```
2501A#config t
2501A(config)#router eigrp 10
2501A(config-router)#network 172.16.0.0
```

2. Start EIGRP on 2501B, and identify the AS number and the directly connected classful networks.

```
2501B#config t
2501B(config)#router eigrp 10
2501B(config-router)#network 172.16.0.0
```

3. Start EIGRP on 2501C, identify the AS number and the directly connected classful networks.

```
2501C#config t
2501C(config)#router eigrp 10
2501C(config-router)#network 172.16.0.0
```

At this point you should be able to ping all the router interfaces. You can also use the `show ip interface brief` command to see the active interfaces and use the `show ip route` command to see all the known routes.

Lab 7.5: Verifying X.25

This lab will provide you with the commands to verify X.25 is configured and running properly on the 2500 routers.

1. Use the `show interface serial 0` command to verify that a connection is made.

```
2501A#show int s0

2501C#show int s0

Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 172.16.20.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation X25, loopback not set
  X.25 DTE, address 3129165551211, state R1, modulo 8, timer 0
      Defaults: idle VC timeout 0
        cisco encapsulation
        input/output window sizes 2/2, packet sizes 128/128
      Timers: T20 180, T21 200, T22 180, T23 180
      Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
      (configuration on Restart: modulo 8,
      Window size: input 2 output 2, Packet size: input 128, output 128
      Channels: Incoming-only none, Two-way 10-100, Outgoing-only none)
      RESTARTs 1/0 CALLs 0+1/0+1/0+0 DIAGs 0/1
  LAPB DTE, state CONNECT, modulo 8, k 7, N1 12056, N2 20
      T1 3000, T2 0, interface outage (partial T3) 0, T4 0
      VS 3, VR 4, tx NR 4, Remote VR 3, Retransmissions 0
      Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
```

```
     IFRAMEs 3/4 RNRs 0/0 REJs 0/0 SABM/Es 1/0 FRMRs 0/0 DISCs 0/0
  Last input never, output 00:00:27, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 4/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7 packets input, 51 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     15 packets output, 1006 bytes, 0 underruns
     0 output errors, 0 collisions, 17 interface resets
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
2501C#

2501C#show int s1

2501B#show int s0
```

2. Use the `show ip route` command to verify your IP routes on all routers.

```
2501A#show ip route

2501C#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
         default
       U - per-user static route, o - ODR

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.30.0 is directly connected, Ethernet0
C       172.16.20.0 is directly connected, Serial0
```

```
2501C#
2501B#show ip route
```

Labs from Chapter 8: Frame Relay

The labs in this section correspond directly with Chapter 8 of the Sybex *CCNP: Remote Access Study Guide*. In these labs you will configure Frame Relay using the 2501B router as the ISP's Frame Relay switch and the 2501A router and 2501B router as the two end points.

To begin these labs, delete any configurations from the routers.

This section includes the following lab exercises:

- Lab 8.1: Deleting the router configurations
- Lab 8.2: Assigning IP addresses to the LAN interfaces of the routers
- Lab 8.3: Configuring Frame Relay with subinterfaces
- Lab 8.4: Enabling EIGRP on the routers
- Lab 8.5: Verifying the Frame Relay configuration

Lab 8.1: Deleting the Router Configurations

In this lab, you will delete the configuration on your routers.

1. Go to the 2501A router and type **erase startup-config**; then reload the router.

   ```
   2501A>ena
   2501A#erase startup-config
   2501A#reload
   ```

2. Go to the 2501B router and type erase **startup-config**; then reload the router.

   ```
   2501B>ena
   2501B#erase startup-config
   2501B#reload
   ```

3. Go to the 2501C router and type erase startup-config; then reload the router.

```
2501C>ena
2501C#erase startup-config
2501C#reload
```

Lab 8.2: Assigning IP Addresses to the LAN Interfaces of the Routers

In this lab, you will configure the basic configuration on your routers. The 2501C router will be the Frame Relay switch and will not be configured with IP addresses, nor will Ethernet 0 interface be part of the network. Configure only the Ethernet interfaces of the 2501A and 2501B routers.

1. Configure the hostname, IP addresses, and enable password for 2501A.

```
Router>enable
Router#config t
Router(config)#enable password cisco
Router(config)#hostname 2501A
2501A(config-if)#interface e0
2501A(config-if)#ip address 172.16.10.1 255.255.255.0
2501A(config-if)#no shutdown
2501A(config-if)#^z
2501A#copy run start
```

2. Configure the hostname, IP addresses, and the enable password for 2501B.

```
Router>enable
Router#config t
Router(config)#enable password cisco
Router(config)#hostname 2501B
2501B(config-if)#interface e0
2501B(config-if)#ip address 172.16.50.1 255.255.255.0
2501B(config-if)#no shutdown
2501B(config-if)#^z
2501B#copy run start
```

Lab 8.3: Configuring Frame Relay with Subinterfaces

The 2501C router will be the Frame Relay switch connecting the 2501A and 2501B routers together using Frame Relay with subinterfaces. The 2501A connection to 2501C will use DLCI 102, and the 2501B-to-2501C connection will use DLCI 201. The subnet 172.16.20.0/24 will be used to make the connection between routers 2501A and 2501B.

1. Configure the 2501C switch with the `frame-relay switching` command, and the encapsulation of each serial interface on the Frame Relay switch (2501C). Also, add the clock rate command to each interface.

```
2501C#config t
2501C(config)#frame-relay switching
2501C(config)#int s0
2501C(config-if)#encapsulation frame-relay
2501C(config-if)#clock rate 64000
2501C(config-if)#int s1
2501C(config-if)#encapsulation frame-relay
2501C(config-if)#clock rate 64000
```

2. Configure the Frame Relay mappings on each interface. You do not need IP addresses on these interfaces because their only task is to switch frames from one interface to another.

```
2501C(config-if)#int s0
2501C(config-if)#frame intf-type dce
2501C(config-if)#frame-relay route 102 interface
   Serial1 201
2501C(config-if)#no shut

2501C(config-if)#int s1
2501C(config-if)#frame intf-type dce
2501C(config-if)#frame-relay route 201 interface
   Serial0 102
2501C(config-if)#no shut
```

This is not as hard as it looks. The `frame-relay route` command just says that if you receive frames from PVC 102, send them out `int s1` using PVC 201. The second mapping on serial 1 is just the opposite. Anything that comes in `int s1` is routed out serial 0 using PVC 102. The `frame intf-type dce` command is required on Frame Relay switching interfaces.

3. Configure the 2501 A with a point-to-point subinterface. Use the IP address 172.16.20.1/24.

```
2501A#config t
2501A(config)#int s0
2501A(config-if)#encapsulation frame-relay
2501A(config-if)#no shut
2501A(config-if)#int s0.102 point-to-point
2501A(config-subif)#ip address 172.16.20.1
   255.255.255.0
2501A(config-subifif)#frame-relay interface-dlci 102
```

4. Configure 2501B with a point-to-point subinterface.

```
2501B#config t
2501B(config)#int s0
2501B(config-if)#encapsulation frame-relay
2501B(config-if)#no shut
2501B(config-if)#int s0.201 point-to-point
2501B(config-subif)#ip address 172.16.20.2
   255.255.255.0
2501B(config-subif)#frame-relay interface-dlci 201
```

Lab 8.4: Enabling EIGRP on the Routers

Configure EIGRP as the routing protocol.

1. Start EIGRP on 2501A, and identify the AS number and the directly connected networks.

```
2501A#config t
2501A(config)#router eigrp 1
2501A(config-router)#network 172.16.0.0
```

2. Start EIGRP on 2501B, and identify the AS number and the directly connected networks.

```
2501B#config t
2501B(config)# router eigrp 1
2501B(config-router)#network 172.16.0.0
```

Lab 8.5: Verifying the Frame Relay Configuration

You can now use ping, trace, and telnet to verify connectivity. You can also use the commands listed below:

Command	Description
`show int`	Displays all the interfaces configured on the router
`show frame-relay pvc`	Displays the configured PVCs
`show running-config`	Displays the current running configuration

1. Use the `show interface` command to verify the Frame Relay information on the serial interfaces.

```
2501A#show interface
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0010.7b81.65bb (bia 0010.7b81.65bb)
  Internet address is 172.16.10.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load
           1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:46, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 510 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     63 packets output, 11692 bytes, 0 underruns
     0 output errors, 0 collisions, 15 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0 is up, line protocol is up
```

```
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
           1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10
           sec)
  LMI enq sent  12, LMI stat recvd 13, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 27/0, interface
           broadcasts 25
  Last input 00:00:03, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     46 packets input, 2706 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     64 packets output, 4127 bytes, 0 underruns
     0 output errors, 0 collisions, 22 interface resets
     0 output buffer failures, 0 output buffers swapped out
     13 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
Serial0.102 is up, line protocol is up
  Hardware is HD64570
  Internet address is 172.16.20.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
           1/255
  Encapsulation FRAME-RELAY
Serial1 is administratively down, line protocol is down
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
           1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
```

```
   Reserved Conversations 0/0 (allocated/max allocated)
  5_minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

2. Verify your configurations with the `show frame-relay` command:

```
2501A#show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0.102

  input pkts 45            output pkts 47           in bytes 3490
  out bytes 3863           dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 38         out bcast bytes 3083
  pvc create time 00:03:20, last time pvc status changed 00:02:44
2501A#
```

3. Use the following command to verify the configuration of each router:

```
2501A#show running-config

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2501A
!
```

```
enable password cisco
!
ip subnet-zero
!
!
!
interface Ethernet0
 ip address 172.16.10.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 no fair-queue
!
interface Serial0.102 point-to-point
 ip address 172.16.20.1 255.255.255.0
 no ip directed-broadcast
 frame-relay interface-dlci 102
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
router eigrp 1
 network 172.16.0.0
!
ip classless
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
end
```

Module 4: CCNP Support Suggested Labs

These labs are designed to help you prepare for and pass the Cisco CCNP Support exam (640-506). The labs follow the new Sybex *CCNP: Support Study Guide*.

These labs can work in conjunction with any study guide or even as a stand-alone product. However, we recommend that you read the Sybex *CCNP: Support Study Guide* since all commands used in these labs are discussed and described in the book.

The following labs are covered in the Support module and are based on topics discussed in detail in the *CCNP: Support Study Guide*:

- Chapter 4: Cisco's Diagnostic Commands
- Chapter 5: Applying Cisco's Diagnostic Tools
- Chapter 7: Troubleshooting Serial Line and Frame Relay Connectivity
- Chapter 8: Troubleshooting ISDN
- Chapter 9: Troubleshooting Novell Connectivity
- Chapter 11: Troubleshooting Switched Ethernet

Labs for Chapter 4: Cisco's Diagnostic Commands

This first section provides the basic suggested lab setup and gathering of information from a router that can be used to diagnose problems on the network. The purpose of this chapter is twofold: to configure the lab used throughout the rest of this program and to introduce you to basic commands used to troubleshoot Cisco routers.

There are 12 labs that are associated with Chapter 4 of Sybex's *CCNP: Support Study Guide*. Remember, the purpose is to introduce the commands, not thoroughly use them at this time.

- Lab 4.1: Gathering the Lab Configuration
- Lab 4.2: Configuring the 2600B Router
- Lab 4.3: Configuring the 2600A Router
- Lab 4.4: Configuring the 5000A Switch
- Lab 4.5: Configuring the 1900A Switch
- Lab 4.6: Configuring the 1900B Switch
- Lab 4.7: Basic Troubleshooting Global Commands
- Lab 4.8: Basic Troubleshooting Interface Commands
- Lab 4.9: Router Process Commands
- Lab 4.10: Debugging Commands
- Lab 4.11: Using the Ping Command
- Lab 4.12: Using the Traceroute Command

Read Chapter 4 of Sybex's *CCNP: Support Study Guide* before performing these labs.

Lab 4.1: Gathering the Lab Configuration

This lab will provide you with the information that you will use throughout the CCNP Support program. Refer to this information as well as the Network Visualizer as much as needed.

Configure the lab in this suggested manner:

2600B

- FastEthernet0/0: 172.16.10.2/24
- Serial0/0: 172.16.50.1/24
- BRI0/0: 172.16.60.1/24
- Serial0/1: Connected to Internet (preconfigured and not configurable)

2600A

- FastEthernet0/0: 172.16.10.1/24
- Serial0/0: 172.16.50.2/24
- BRI0/0: 172.16.60.2/24

5000A

- IP address: 172.16.10.3/24
- 1/1 Connection to 2600A Fa0/0
- 1/2 Connection to 2600B Fa0/0
- 2/1 Connection to 1900A F0/26
- 2/2 Connection to 1900B F0/26

1900A

- IP Address: 172.16.10.5/24
- F0/26 connected to 5000A 2/1
- E0/1 connected to HostA
- E0/2 connected to HostB

1900B

- IP Address 172.16.10.4/24
- F0/26 connected to 5000A 2/2
- E0/1 connected to HostC

HostA

- Preconfigured to 172.16.10.6/24

HostB

- Preconfigured to 172.16.20.2/24

HostC

- Preconfigured to 172.16.30.2/24

Lab 4.2: Configuring the 2600B Router

This lab will provide the suggested lab configuration of the 2600B router.

1. Configure the 2600B router with the hostname, passwords, and banner.

```
Router>enable
Router#config t
Router(config)#hostname 2600B
2600B(config)#enable secret todd
2600B(config)#line console 0
2600B(config-line)#login
2600B(config-line)#password bill
2600B(config-line)#line vty 0 4
2600B(config-line)#login
2600B(config-line)#password julie
2600B(config-line)#exit
2600B(config)#banner motd #
2600B(config)#Enter text message. End with the
   character '#'
This is the 2600B router
#
2600B(config)#
```

2. Configure the 2600B router with interface IP addresses and descriptions, and enable the interfaces. The serial 0 interface is a DCE interface, so configure it appropriately. (Do not configure the BRI interface at this time.)

```
2600B(config)#int fastethernet 0/0
2600B(config-if)#ip address 172.16.10.2 255.255.255.0
2600B(config-if)#description connection to 5000A
2600B(config-if)#no shut
2600B(config-if)#interface serial 0/0
2600B(config-if)#ip address 172.16.50.1 255.255.255.0
2600B(config-if)#description connection to 2600A
2600B(config-if)#clock rate 64000
2600B(config-if)#no shut
2600B(config-if)#exit
2600B(config-if)#^z
2600B#copy running-config startup-config
2600B#
```

You can also type **copy run start** when saving your configurations.

Lab 4.3: Configuring the 2600A Router

This section provides you with the suggested lab configuration of the 2600A router.

1. Configure the 2600A router with the hostname, passwords, and banner.

```
Router>enable
Router#config t
Router(config)#hostname 2600A
2600A(config)#enable secret todd
2600A(config)#line console 0
2600A(config-line)#login
2600A(config-line)#password bill
2600A(config-line)#line vty 0 4
2600A(config-line)#login
2600A(config-line)#password julie
2600A(config-line)#exit
2600A(config)#banner motd #
This is the 2600A router
#
2600A(config)#
```

2. Configure the 2600A router with interface IP addresses and descriptions, and enable the interfaces. (Do not configure the BRI interface at this time.)

```
2600A(config)#int fastethernet 0/0
2600A(config-if)#ip address 172.16.10.1 255.255.255.0
2600A(config-if)#description  connection to 5000A
2600A(config-if)#no shut
2600A(config-if)#interface serial 0/0
2600A(config-if)#ip address 172.16.50.2 255.255.255.0
2600A(config-if)#description  connection to 2600B
2600A(config-if)#no shut
2600A(config-if)#exit
2600A(config-if)#^z
2600A#copy running-config startup-config
2600A#
```

Lab 4.4: Configuring the 5000A Switch

This section provides the suggested lab configuration of the 5000A switch.

1. Configure the 5000A switch with a hostname, passwords, and banner.

```
Enter password: [press enter]
Console>enable
Console>(enable)set prompt 5000A>
5000A>(enable)set password
Enter old password:
Enter new password: todd
Retype new password: todd
5000A>(enable)set enablepass
Enter old password:
Enter new password: cisco
Retype new password: cisco
5000A>(enable)set banner motd #
This is the 5000A switch
#
5000A>(enable)
```

2. Configure the 5000A switch with an IP address, a default-gateway, and interface descriptions.

```
5000A>(enable)set int sc0 172.16.10.3 255.255.255.0
5000A>(enable)set ip route 0.0.0.0 172.16.10.1
5000A>(enable)set port name 1/1 To 2600A
5000A>(enable)set port name 1/2 To 2600B
5000A>(enable)set port name 2/1 To 1900A
5000A>(enable)set port name 2/2 To 1900B
```

Lab 4.5: Configuring the 1900A Switch

This section provides the suggested lab configuration of the 1900A switch.

1. Configure the 1900A switch with a hostname, password, and banner.

```
>enable
#config t
(config)#hostname 1900A
1900A(config)#enable secret todd
1900A(config)#banner motd #
```

```
1900A(config)#Enter text message. End with the
   character '#'
This is the 1900A switch
#
1900A(config)#
```

2. Configure the 1900A switch with an IP address, a default-gateway, and interface descriptions.

```
1900A(config)#ip address 172.16.10.5 255.255.255.0
1900A(config)#ip default-gateway 172.16.10.1
1900A(config)#interface fastethernet 0/26
1900A(config-if)#description connection_to_5000A
1900A(config-if)#interface e/01
1900A(config-if)#description connection_to_HostA
1900A(config-if)#interface e0/2
1900A(config-if)#description connection_to_HostB
1900A(config-if)#^z
1900A#
```

Lab 4.6: Configuring the 1900B Switch

This section provides the suggested lab configuration of the 1900A switch.

1. Configure the 1900B switch with a hostname, password, and banner.

```
>enable
#config t
(config)#hostname 1900B
1900B(config)#enable secret todd
1900B(config)#banner motd #
1900B(config)#Enter text message. End with the
   character '#'
This is the 1900B switch
#
1900B(config)#
```

2. Configure the 1900B switch with an IP address, a default-gateway, and interface descriptions.

```
1900B(config)#ip address 172.16.10.4 255.255.255.0
1900B(config)#ip default-gateway 172.16.10.1
1900B(config)#interface fastethernet 0/26
1900B(config-if)#description connection_to_5000A
```

```
1900B(config-if)#interface e0/1
1900B(config-if)#description connection_to_ HostC
1900B(config-if)#^z
1900B#
```

Lab 4.7: Basic Troubleshooting Global Commands

This lab will describe how to use some basic commands to troubleshoot a Cisco internetwork. The commands in this lab are called *global commands* because they provide information about the router as a whole. All of these commands can be used throughout the rest of the labs in the CCNP Support program. The purpose of the labs throughout this section is to introduce you to the commands. In later sections you will use these commands with the associated labs.

1. From the 2600B router, type **show ?** to see the large number of commands supported by Cisco, and verify your configuration.

```
2600B#show ?
  access-expression  List access expression
  access-lists       List access lists
  accounting         Accounting data for active sessions
  adjacency          Adjacent nodes
  aliases            Display alias commands
  alps               Alps information
  apollo             Apollo network information
  appletalk          AppleTalk information
  arap               Show Appletalk Remote Access statistics
  arp                ARP table
  async              Information on terminal lines used as
                     router interfaces
  backup             Backup status
  bridge             Bridge Forwarding/Filtering Database
                     [verbose]
  bsc                BSC interface information
  bstun              BSTUN interface information
  buffers            Buffer pool statistics
  c2600              Show c2600 information
  call               Show Calls
  cdp                CDP information
```

```
cef                 Cisco Express Forwarding
clns                CLNS network information
clock               Display the system clock
cls                 DLC user information
compress            Show compression statistics
configuration       Contents of Non-Volatile memory
context             Show context information
controllers         Interface controller status
debugging           State of each debugging option
decnet              DECnet information
dhcp                Dynamic Host Configuration Protocol status
diag                Show diagnostic information for port
                    adapters/modules
dial-peer           Dial Plan Mapping Table for, e.g. VoIP
                    Peers
dialer              Dialer parameters and statistics
dialplan            Voice telephony dial plan
dlsw                Data Link Switching information
dnsix               Shows Dnsix/DMDP information
drip                DRiP DB
dspu                Display DSPU information
dxi                 atm-dxi information
entry               Queued terminal entries
environment         Environmental monitor statistics
exception           exception informations
file                Show filesystem information
flash:              display information about flash: file
                    system
frame-relay         Frame-Relay information
fras                FRAS Information
fras-host           FRAS Host Information
gateway             Show status of gateway
history             Display the session command history
hosts               IP domain-name, lookup style, nameservers,
                    and host table
html                HTML helper commands
interfaces          Interface status and configuration
ip                  IP information
ipx                 Novell IPX information
isdn                ISDN information
```

```
isis                IS-IS routing information
kerberos            Show Kerberos Values
key                 Key information
keymap              Terminal keyboard mappings
lat                 DEC LAT information
line                TTY line information
llc2                IBM LLC2 circuit information
lnm                 IBM LAN manager
local-ack           Local Acknowledgement virtual circuits
location            Display the system location
logging             Show the contents of logging buffers
memory              Memory statistics
modemcap            Show Modem Capabilities database
nbf                 NBF (NetBEUI) information
ncia                Native Client Interface Architecture
netbios-cache       NetBIOS name cache contents
node                Show known LAT nodes
ntp                 Network time protocol
num-exp             Number Expansion (Speed Dial) information
pas                 Port Adapter Information
pci                 PCI Information
ppp                 PPP parameters and statistics
printers            Show LPD printer information
privilege           Show current privilege level
processes           Active process statistics
protocols           Active network routing protocols
qllc                Display qllc-llc2 and qllc-sdlc conversion
                    information
queue               Show queue contents
queueing            Show queueing configuration
registry            Function registry information
reload              Scheduled reload information
rhosts              Remote-host+user equivalences
rif                 RIF cache entries
rmon                rmon statistics
route-map           route-map information
rtr                 Response Time Reporter (RTR)
running-config      Current operating configuration
sdllc               Display sdlc - llc2 conversion information
services            LAT learned services
```

sessions	Information about Telnet connections
sgbp	SGBP group information
smds	SMDS information
smf	Software MAC filter
smrp	Simple Multicast Routing Protocol (SMRP) information
sna	Display SNA host information
snapshot	Snapshot parameters and statistics
snmp	snmp statistics
source-bridge	Source-bridge parameters and statistics
spanning-tree	Spanning tree topology
sscop	SSCOP
stacks	Process stack utilization
standby	Hot standby protocol information
startup-config	Contents of startup configuration
stun	STUN status and configuration
subscriber-policy	Subscriber policy
subsys	Show subsystem information
tacacs	Shows tacacs+ server statistics
tarp	TARP information
tcp	Status of TCP connections
tech-support	Show system information for Tech-Support
terminal	Display terminal configuration parameters
time-range	Time range
tn3270	TN3270 settings
traffic-shape	traffic rate shaping configuration
translate	Protocol translation information
ttycap	Terminal capability tables
users	Display information about terminal lines
version	System hardware and software status
vines	VINES information
vlans	Virtual LANs Information
voice	Voice port configuration & stats
vpdn	VPDN information
whoami	Info on current tty line
x25	X.25 information
x29	X.29 information
xns	XNS information
xremote	XRemote statistics

You can see there are a lot of commands. We will go through the most important commands now.

2. The `show version` command is used to display the system hardware and software versions. It also includes information about how long the router was running and the reason it was last restarted. Let's look at the output of the `show version` command.

```
2600B#show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JS-M), Version
   12.0(3)T3,  RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 15-Apr-99 17:05 by kpma
Image text-base: 0x80008088, data-base: 0x80C2D514
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE
   SOFTWARE (fc1)
2600B uptime is 13 minutes
System restarted by power-on
System image file is "flash:c2600-js-mz.120-3.T3.bin"
cisco 2621 (MPC860) processor (revision 0x101) with
   24576K/8192K bytes of memory
Processor board ID JAB0402040J (2308906173)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology
   Corp.
TN3270 Emulation software.
Basic Rate ISDN software, Version 1.1.
2 FastEthernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

At the very end of the `show version` command, the configuration-register setting is shown. This tells the router how to boot.The value `0x2102` tells the router to load the IOS from flash and then load the configuration from NVRAM.

3. The `show running-config` and `show startup-config` commands are used to view the syntax of the router's configuration. The `show startup-config` command displays the contents of the configuration that was written to NVRAM. The `show running-config` command displays the configuration that was loaded into memory and is running on the router. (The `show running-config`, `show config`, and `write term` commands are equivalent.)

```
2600B#show running-config
2600B#show startup-config
```

4. The `show logging` command can provide the first indication of a network problem. There are six types of logging: syslog, console, monitor, trap, buffer, and SNMP. Each may be logged to the console or to a syslog or SNMP server. Following is the output from the `show logging` command:

```
2600B#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes,
   0 overruns)
    Console logging: level debugging, 18 messages logged
    Monitor logging: level debugging,  0 messages logged
     Buffer logging: disabled
     Trap logging: level informational,22 message lines
       logged
```

The output simply tells us that syslog, console, monitor, trap, buffer, and SNMP are all enabled. If they are not enabled, the output indicates the status. It gives some statistical information about the number of messages logged and where they are logged.

5. The `show stacks` command is not very useful to you, but it is invaluable information for the Cisco TAC. The output from the command follows. As you can see, it doesn't make a lot of sense to the user. The information is sent to Cisco, and Cisco runs it through a stack decode that provides the information relevant to system problems.

```
2600B#show stacks
Minimum process stacks:
 Free/Size   Name
10336/12000  Init
 5380/6000   RADIUS INITCONFIG
 8456/9000   DHCP Client

Interrupt level stacks:
Level Called  Unused/Size Name
1     510     8612/9000   Network interfaces
2     0       9000/9000   Timebase Reference Interrupt
3     0       9000/9000   PA Management Int Handler
```

```
6      319      8884/9000    16552 Con/Aux Interrupt
7      229380   8916/9000    MPC860 TIMER INTERRUPT
```

6. The `tech-support` command is a compilation of several `show` commands (`version`, `running-config`, `controllers`, `stacks`, `interfaces`, `diagbus`, `buffers`, `process memory`, `process cpu`, `context`, `boot`, `flash bootflash`, `ip traffic`, and `controllers cbus`). You can get most of the information you need by issuing the `show tech-support` command, instead of issuing all of the commands separately.

   The `tech-support` command does not allow you to scroll through it on the router because of the enormous amount of information that is displayed. To capture the output, you need a terminal with a large line buffer setting, or you can log the output directly to a terminal.

   ```
   2600B#show tech-support
   ```

7. The `show memory` command is helpful for diagnosing memory problems (such as allocation failures, free memory, and so on).

   ```
   2600B#show memory
   ```

   The fields you'll see as a result of this are self-explanatory; they describe the total, used, and free amounts of memory. The second field gives detailed information concerning the memory allocation and utilization. The most relevant information is contained in the first field.

8. The buffers are used to store packets that are waiting to be processed by the CPU. The buffers come configured with default settings. They can be modified, if necessary, but it is usually a good idea to have a Cisco TAC engineer look at the memory allocation and suggest the new buffer settings. To see an example of the buffer settings from the 2600B router, type in the `show buffers` command from privileged mode:

   ```
   2600B#show buffers
   ```

   The 2600 series of routers shows the interface buffers at the end of this command.

Lab 4.8: Using Basic Troubleshooting Interface Commands

Interface commands deal with detailed interface settings and configurations. Because each type of interface uses different protocols and technologies, the `show interface` command is capable of displaying all data related to the specified interface.

The `show interface` command has many derivatives. A simple `show interface` command can be issued, and you will get the detailed status and configuration of every interface on the router. That can be overwhelming—so many options exist for the command. These options allow you, the engineer, to focus the area of your troubleshooting.

1. Type **`show interface`** from the privileged mode of the 2600B router.

   ```
   2600B#show interface
   ```

   You can also type **`show interface fastethernet 0/0`** to get only the specific configuration of Fastethernet 0/0.

   ```
   2600B#show interface  fastethernet 0/0
   ```

   The output you'll see starts with the most pertinent information: the physical interface and line protocol status. In this case, you'll see that both are up. There is much argument as to what constitutes an "up" interface. It is very simple: the controller sends a signal that there are electrons flowing through the physical interface. So just doing a `no shut` on an interface brings it into an "up" status, even if nothing is plugged into the interface. Line protocol "up" means that the interface is able to send itself a frame and receive it back.

2. Use the `show interface serial 0/0` command to see the statistics of the serial interface.

```
2600B#show interface serial 0/0

Serial0/0 is up, line protocol is down
  Hardware is PowerQUICC Serial
  Description: Connection to 2600A
  Internet address is 172.16.50.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliablility 253/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     13 packets input, 172 bytes, 0 no buffer
     Received 7 broadcasts, 0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 2 frame, 0 overrun, 0 ignored, 0 abort
     31 packets output, 4207 bytes, 0 underruns
     0 output errors, 0 collisions, 33 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
4 carrier transitions
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

HDLC is used by default on Cisco serial interfaces. The first important point of troubleshooting serial line problems is to verify that both sides of the link are using the same encapsulation types. Notice the line in the previous output that shows the encapsulation method.

3. The router will keep a table of IP addresses resolved to a hardware address called an ARP table. Then, the next time that the router wants to speak with the given machine, it uses the ARP table instead of broadcasting an ARP packet. Use the `show ip arp` command for a look at the ARP table:

   ```
   2600B#show ip arp
   ```

   When you view the output, notice that the 2600A and the 5000A are both in the ARP table because the 2600B is directly attached to the same LAN. ARP entries time out after 4 hours by default on Cisco routers.

4. The `show interfaces accounting` command simply tracks the protocol traffic on an interface. It counts the number of packets in and out, as well as the number of characters. Here is a sample output:

```
2600B#show interfaces accounting

FastEthernet0/0 Connection to 5000A
Protocol    Pkts In   Chars In   Pkts Out  Chars Out
  IP          0          0         37       12930
 ARP          1         60         11         660
 CDP          2        366         14        4133
Serial0/0 Connection to 2600A
Protocol    Pkts In   Chars In   Pkts Out  Chars Out
  IP          0          0         37       12930
 CDP          0          0         12        2603
Interface BRI0/0 is disabled

Interface BRI0/0:1 is disabled

Interface BRI0/0:2 is disabled

Interface FastEthernet0/1 is disabled
```

Lab 4.9: Router Process Commands

There are two very important process commands that can be executed. Process commands deal directly with the process running on the router. If the standard `show processes` command is issued, you get a result similar to a `ps -ef` executed on a Unix box. The output details each process, process ID number (PID), time running, and stack information. The output is too general to be used effectively while troubleshooting.

The two options available with the `show processes` command are `cpu` and `memory`. Each of these options refines the output and makes it more useful and user-friendly.

1. The command `show processes cpu` relates the router's processes and CPU utilization. The first line of the output displays the router's CPU utilization over three time frames.

```
2600B#show processes cpu
2600B#show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
   1           0       75      0   0.00%  0.00%  0.00%   0 Load Meter
   2        2100     1407   1492   0.00%  0.24%  0.64%   0 Exec
   3         384       57   6736   0.00%  0.08%  0.04%   0 Check heaps
   4           0        1      0   0.00%  0.00%  0.00%   0 Pool Manager
   5           0        2      0   0.00%  0.00%  0.00%   0 Timers
   6           0        2      0   0.00%  0.00%  0.00%   0 Serial Background
   7           0       14      0   0.00%  0.00%  0.00%   0 Environmental mo
   8           0       24      0   0.00%  0.00%  0.00%   0 ARP Input
   9           0        4      0   0.00%  0.00%  0.00%   0 DDR Timers
  10           0        2      0   0.00%  0.00%  0.00%   0 Dialer event
  11           4        2   2000   0.00%  0.00%  0.00%   0 Entity MIB API
  12           0        1      0   0.00%  0.00%  0.00%   0 SERIAL A'detect
  13           0        1      0   0.00%  0.00%  0.00%   0 Critical Bkgnd
  14          28       70    400   0.00%  0.00%  0.00%   0 Net Background
  15           4       10    400   0.00%  0.00%  0.00%   0 Logger
  16          12      368     32   0.00%  0.00%  0.00%   0 TTY Background
  17           0      479      0   0.00%  0.00%  0.00%   0 Per-Second Jobs
  18           0      372      0   0.00%  0.00%  0.00%   0 Partition Check
  19           0       31      0   0.00%  0.00%  0.00%   0 Net Input
  20           0       76      0   0.00%  0.00%  0.00%   0 Compute load avg
  21         192        9  21333   0.00%  0.04%  0.00%   0 Per-minute Jobs
 PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
  22           8       53    150   0.00%  0.00%  0.00%   0 IP Input
```

```
 23           4          49       81  0.00%  0.00%  0.00%    0 CDP Protocol
 24           0           1        0  0.00%  0.00%  0.00%    0 Asy FS Helper
 25           0           1        0  0.00%  0.00%  0.00%    0 PPP IP Add Route
 26           0           3        0  0.00%  0.00%  0.00%    0 MOP Protocols
 27           0           1        0  0.00%  0.00%  0.00%    0 X.25 Encaps Mana
 28           4          38      105  0.00%  0.00%  0.00%    0 IP Background
 29           0           2        0  0.00%  0.00%  0.00%    0 SSCOP Input
 30           0           2        0  0.00%  0.00%  0.00%    0 SSCOP Output
 31           4           9      444  0.00%  0.00%  0.00%    0 SSCOP Timer
 32           0           2        0  0.00%  0.00%  0.00%    0 ILMI Input
 33           0           1        0  0.00%  0.00%  0.00%    0 SNMP Timers
 34           0           2        0  0.00%  0.00%  0.00%    0 ILMI Request
 35           0           2        0  0.00%  0.00%  0.00%    0 ILMI Response
 36           0           1        0  0.00%  0.00%  0.00%    0 ILMI Timer Proce
 37           0           2        0  0.00%  0.00%  0.00%    0 ATM PVC Discover
 38           0           1        0  0.00%  0.00%  0.00%    0 TCP Timer
 39           0           1        0  0.00%  0.00%  0.00%    0 TCP Protocols
 40           4           1     4000  0.00%  0.00%  0.00%    0 Probe Input
 41           0           4        0  0.00%  0.00%  0.00%    0 RARP Input
 42           0           1        0  0.00%  0.00%  0.00%    0 Socket Timers
 43           8           6     1333  0.00%  0.00%  0.00%    0 DHCPD Receive
PID  Runtime(ms)     Invoked    uSecs   5Sec   1Min   5Min TTY Process
 44           0           8        0  0.00%  0.00%  0.00%    0 IP Cache Ager
 45           0           1        0  0.00%  0.00%  0.00%    0 PAD InCall
 46           4           3     1333  0.00%  0.00%  0.00%    0 X.25 Background
 47           0           9        0  0.00%  0.00%  0.00%    0 TCP Intercept Ti
 48           0           2        0  0.00%  0.00%  0.00%    0 SPX Input
 49           0           8        0  0.00%  0.00%  0.00%    0 Adj Manager
 50           0           2        0  0.00%  0.00%  0.00%    0 ALPS P1024_CktMg
 51           0           2        0  0.00%  0.00%  0.00%    0 ALPS X.25 Ckt Mg
 52           0           1        0  0.00%  0.00%  0.00%    0 ISDN Timer
 53           0           1        0  0.00%  0.00%  0.00%    0 Time Range Proce
 54           0           1        0  0.00%  0.00%  0.00%    0 IP NAT Ager
 55           4           2     2000  0.00%  0.00%  0.00%    0 CC-API_VCM
 56           4           2     2000  0.00%  0.00%  0.00%    0 Session Applicat
 57           0           1        0  0.00%  0.00%  0.00%    0 CCVPM_HDSPRM
 58           0           2        0  0.00%  0.00%  0.00%    0 Voice Player
 59           0           1        0  0.00%  0.00%  0.00%    0 pcapp
 60           0           1        0  0.00%  0.00%  0.00%    0 placecall
 61           0           1        0  0.00%  0.00%  0.00%    0 ivr app
```

```
  62           0           1       0   0.00%   0.00%   0.00%   0 ivr app
  63           0           1       0   0.00%   0.00%   0.00%   0 ivr app
  64           4           1    4000   0.00%   0.00%   0.00%   0 ivr app
  65           0           1       0   0.00%   0.00%   0.00%   0 ivr app
 PID  Runtime(ms)   Invoked   uSecs    5Sec    1Min    5Min TTY Process
  66           0           1       0   0.00%   0.00%   0.00%   0 ivr app
  67           0           1       0   0.00%   0.00%   0.00%   0 ivr app
  68           0           1       0   0.00%   0.00%   0.00%   0 CCVPM_HTSP
  69           0           1       0   0.00%   0.00%   0.00%   0 VTSP
  70           0           1       0   0.00%   0.00%   0.00%   0 ISDNMIB Backgrou
  71           0           1       0   0.00%   0.00%   0.00%   0 CallMIB Backgrou
  72           0           1       0   0.00%   0.00%   0.00%   0 SNMP ConfCopyPro
  73           0           1       0   0.00%   0.00%   0.00%   0 Syslog Traps
  74           0          11       0   0.00%   0.00%   0.00%   0 IP-RT Background
  76           8           2    4000   0.00%   0.00%   0.00%   0 CCH323_CT
  77           0           2       0   0.00%   0.00%   0.00%   0 CCH323_RTCP
  78           0           1       0   0.00%   0.00%   0.00%   0 CCH323_DNS
  79           0           1       0   0.00%   0.00%   0.00%   0 CCH323_SOCKET
  81           0           4       0   0.00%   0.00%   0.00%   0 DHCPD Timer
  83           0           2       0   0.00%   0.00%   0.00%   0 CCP manager
  84           0           2       0   0.00%   0.00%   0.00%   0 PPP manager
  85           4         380      10   0.00%   0.00%   0.00%   0 Multilink PPP
  86           0           2       0   0.00%   0.00%   0.00%   0 Multilink PPP ou
  87           0           2       0   0.00%   0.00%   0.00%   0 Multilink event
  88           0           4       0   0.00%   0.00%   0.00%   0 FR LMI
  89           0           1       0   0.00%   0.00%   0.00%   0 FR ARP
  90           0        4699       0   0.00%   0.00%   0.00%   0 FR Broadcast Out
 PID  Runtime(ms)   Invoked   uSecs    5Sec    1Min    5Min TTY Process
  91           0          24       0   0.00%   0.00%   0.00%   0 FR TUNNEL
  92           0           1       0   0.00%   0.00%   0.00%   0 FRF9 manager
  93           0         104       0   0.00%   0.00%   0.00%   0 DHCPD Database
2600B#
```

2. The second option, `show processes memory`, is used to associate memory utilization with the router's processes.

   `2600B#show processes memory`

   The first line you'll see details the total, used, and free amounts of system memory. Following that, you'll see the PID, allocated, freed, and holding memory. This means that the processor has allocated a given amount of memory to the process; if the process does not need all of that memory, it frees some of it and retains the rest.

Lab 4.10: Debugging Commands

Debugging commands are used to show an administrator the packets as they cross the CPU of the router. This is an invaluable tool, and one we will use often with this program.

1. First, make sure that your router is configured to apply timestamps to all messages. This is done with the following commands:
   - `service timestamps debug datetime msec localtime`
   - `service timestamps log datetime msec localtime`

   Here is an example:

```
2600B>enable
2600B#config t
2600B(config)#service timestamps debug datetime msec
   localtime
2600B(config)#service timestamps log datetime msec
   localtime
2600B(config)#exit
2600B#
```

2. Make sure that you see the debug messages. By default, error and debug messages are sent only to the console. If you are telneted to the router, you do not see the debug or log messages unless you issue the following command:

```
2600B#terminal monitor
```

   You can turn messages off by issuing the "no" form of the command.

```
2600B#terminal no monitor
```

3. To obtain a comprehensive list of `debug` commands, issue the following command:

```
2600B#debug ?
```

4. To stop the debug process, the easiest way is to type the following command:

```
2600B#undebug all
```

   However, the shortcut `un all` works just as well; it is short and sweet, yet effective.

5. Practice with a debugging command, and we'll go through more of the debugging commands in later sections.

```
2600B#debug ip packet
2600B#undebug all
```

Lab 4.11: Using the Ping Command

The previous tools are in-depth tools used for problems that require very high granularity. This means that these tools are used to provide very detailed and specific information at a very low-level view. The `ping` command is a high-level, simple tool. It is used to test for reachability and connectivity throughout a network.

IP `ping` uses ICMP as the protocol to provide connectivity and reachability messages. It works on a simple principle: an ICMP echo message is sent to the specified IP address. If the address is reachable, the receiving station sends an ICMP echo-reply message back to the sending station.

1. From the 2600B router, ping the 2600A Fa0/0 interface. The `ping` command can be used at either privileged or usermode EXEC mode.

```
2600B#ping 172.16.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.10.1, timeout
   is 2    seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
   min/avg/max =    1/2/4 ms
2600B#
```

2. Exclamation points (!) mean a response from the destination.
3. Ping an address that does not exist to see the output.

```
2600B#ping 172.16.2.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.2.130, timeout
   is    2 seconds:
.....
Success rate is 0 percent (0/5)
2600B#
```

   In the first ping, all five packets received echo-reply messages, which indicates that the host is reachable. Notice that the output gives a success percentage based on the five requests that were sent. It also gives the minimum, average, and maximum response times.
   The second ping doesn't look so good. All five requests timed out. This means that each request waited two seconds for a response. When no response was received, a "." was echoed to the screen. It is possible that a request was received, but it was after the two-second waiting period. Either way, the host cannot be considered reachable.
4. The 2600B router is connected to the Internet. From the 2600B, ping to a Web site on the Internet. This lab will use `www.routersim.com` as an example. (Besides, why would you want to go anywhere else?)

```
2600B#ping www.routersim.com

Pinging routersim.com [64.70.169.57] with 32 bytes of
   data:

Reply from 64.70.169.57: bytes=32 time=822ms TTL=241
Reply from 64.70.169.57: bytes=32 time=210ms TTL=241
Reply from 64.70.169.57: bytes=32 time=761ms TTL=241
Reply from 64.70.169.57: bytes=32 time=210ms TTL=241

Ping statistics for 64.70.169.57:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 210ms, Maximum =  822ms, Average =  500ms

2600B#
```

This is a limited lab and will only work if you go to `www.routersim.com` and `www.globalnettraining.com`, because this is a simulated product.

Lab 4.12: Using the *traceroute* Command

The `traceroute` command is used to show an administrator the path a packet takes as it traverses a network looking for a destination host, unlike the `ping` command, which tells the administrator if a host has IP connectivity.

1. Practice using the `traceroute` command by issuing the following command from the 2600B router to `www.routersim.com`:

```
2600B#traceroute www.routersim.com
Tracing route to routersim.com [64.70.169.57]
over a maximum of 30 hops:
 1   130 ms   120 ms   120 ms  tnt1.dillon.co.da.uu.net [206.115.223.53]
 2   722 ms   120 ms   120 ms  206.115.235.241
 3   130 ms   170 ms   131 ms  ar1.den2.da.uu.net [207.76.12.131]
 4   130 ms   120 ms   131 ms  173.Serial2-1-1.GW1.DEN1.ALTER.NET [137.39.68.202]
 5   150 ms   811 ms   141 ms   114.at-5-0-0.XR1.SLT4.ALTER.NET [146.188.224.106]
 6   671 ms   131 ms   140 ms  187.at-1-0-0.TR1.SLT4.ALTER.NET [152.63.89.18]
 7   701 ms   161 ms   170 ms  133.at-5-1-0.TR1.DFW9.ALTER.NET [152.63.5.42]
```

```
 8   801 ms   160 ms   171 ms  0.so-3-0-0.XR1.DFW9.ALTER.NET [152.63.10.14]
 9   711 ms   171 ms   170 ms  185.ATM5-0.BR3.DFW9.ALTER.NET [152.63.100.161]
10   661 ms   170 ms   171 ms  137.39.52.50
11   170 ms   171 ms   170 ms  gbr3-p50.dlstx.ip.att.net [12.123.16.242]
12   200 ms   190 ms   191 ms  gbr4-p20.attga.ip.att.net [12.122.2.90]
13   211 ms   210 ms   190 ms  gbr3-p60.attga.ip.att.net [12.122.1.141]
14   731 ms   200 ms   190 ms  gbr4-p50.ormfl.ip.att.net [12.122.2.130]
15   200 ms   190 ms   201 ms  gbr1-p90.ormfl.ip.att.net [12.122.5.126]
16   752 ms   200 ms   200 ms  ar5-p310.ormfl.ip.att.net [12.123.32.90]
17   211 ms   200 ms   721 ms  12.126.145.42
18   801 ms   211 ms   230 ms  ftl-core1a-v5.valueweb.com [216.219.251.1]
19   771 ms   210 ms   211 ms  routersim.com [64.70.169.57]

Trace complete.

2600B#
```

This is a limited lab and the `traceroute` command will only work if you go to `www.routersim.com` and `globalnettraining.com`, because this is a simulated product. Notice that `www.routersim.com` was 19 hops from our source router. The domain name is displayed on any IP address that could be looked up in a name server.

Labs from Chapter 5: Applying Cisco's Diagnostic Tools

In this section a bug will be applied into both the 2600B and 2600A routers. You will need to diagnose the problem using the commands you learned in the previous section. You will perform the following labs:

- Lab 5.1: Testing your Network Configuration
- Lab 5.2: Bugging and Troubleshooting

Before you continue into this chapter, be sure that you have configured the network from Lab 4.1.

Lab 5.1: Testing Your Network Configuration

This lab will help you verify your network configuration, which is imperative before you introduce bugs into the network.

1. From the 2600B router, ping to all devices except hosts B and C, which will not work at this time.

   ```
   2600B#ping 172.16.10.1
   2600B#ping 172.16.10.3
   2600B#ping 172.16.10.4
   2600B#ping 172.16.10.5
   2600B#ping 172.16.10.6
   2600B#ping 172.16.50.2
   ```

   If any of these are unsuccessful, your first assignment is to troubleshoot the problem and fix it. You should also be able to ping from any other device to the 2600B router.

2. Continue to verify your network by simultaneously telneting into all devices from the 2600B router. You cannot telnet into the hosts. After you telnet into a router or switch, press Control+Shift+6, let go, and then press the X key. This will take you back to the 2600B router console. From there, telnet into the next device.

   ```
   2600B#telnet 172.16.10.1
   2600B#telnet 172.16.10.3
   2600B#telnet 172.16.10.4
   2600B#telnet172.16.10.5
   ```

3. After you have finished telneting into all devices, type the following to see the open sessions.

   ```
   2600B#show sessions
   ```

   You can return to any session by typing the number to the left of the desired session and pressing return twice.

If you can both ping and telnet throughout the network, you have successfully configured the network and can now continue on to the next lab exercise.

Lab 5.2: Bugging and Troubleshooting

This lab will have you introduce bugs into the 2600A and 2600B routers and then diagnose, troubleshoot and fix the problem. Only after you can run through lab 5.2 successfully again is this lab complete. The idea is to make the network configuration work and look *exactly* as it is in lab 4.1.

1. In the lab screen in the program, click the Implement Bugs button.
2. Go through the basic commands to find the problem. (See if you can fix this without looking at the running-config.)

   A. First, check your IP connectivity by pinging.

   B. Find the areas that do not work.

   C. Login into each router and run your show commands.

   D. Do the `show running-config` last if possible.

   E. Fix the problems.

   The problems were simple, but not always easy to see. For example, the 2600B router has a prompt that says Router(boot); this indicates a IOS problem. However, by using the `show flash` command and `show version` command, you should have seen that the problem was not the IOS.

Here are the problems you should have fixed:

For the 2600A router:

- Change the hostname back to 2600A.
- Set the banner.
- Set the enable secret.
- Change the duplicate IP address on interface fa0/0 back to 172.16.10.1 255.255.255.0.
- Change the keep-alive time on serial 0/0 back to 10.

For the 2600B router:

- Change the hostname back to 2600B.
- Set the banner.
- Set the enable secret.
- Change the interface encapsulation back to HDLC from PPP.

Labs from Chapter 7: Troubleshooting Serial Line and Frame Relay Connectivity

This section will help you troubleshoot WAN connectivity using point-to-point serial links and Frame Relay. The labs in this section will have you verify your connection between the 2600B and 2600A routers using HDLC and Frame Relay.

Before you attempt this lab, make sure the network is configured according to Lab 4.1 and that you can both ping and telnet throughout the network. You will perform the following labs:

- Lab 7.1: Verifying Serial Line Connectivity
- Lab 7.2: Bugging and Troubleshooting Serial Links
- Lab 7.3: Configuring Frame Relay
- Lab 7.4: Verifying Frame Relay Connectivity
- Lab 7.5: Bugging and Troubleshooting Frame Relay

Read Chapter 7 of Sybex's *CCNP: Support Study Guide* before attempting the labs in this section.

Lab 7.1: Verifying Serial Line Connectivity

This lab has you verify your existing network configuration between the 2600B and 2600A router.

There are numerous commands available to aid in troubleshooting serial lines. Some of them are `show` commands; others are `debug` commands. Here is a list of the commands that will be covered in this section:

```
show interface serial
clear counters serial
show controllers serial
debug serial interface
debug serial packet
```

1. Connect to the 2600B router from the Network Visualizer and log in. From either the usermode or privileged mode prompt, type **show interface serial 0/0**.

```
2600B>show interface serial 0/0

Serial0/0 is up, line protocol is down
  Hardware is PowerQUICC Serial
  Description: Connection to 2600A
  Internet address is 172.16.50.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliablility 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     64 packets input, 845 bytes, 0 no buffer
     Received 38 broadcasts, 0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 2 frame, 0 overrun, 0 ignored, 0 abort
     81 packets output, 14433 bytes, 0 underruns
     0 output errors, 0 collisions, 40 interface resets
     0 output buffer failures, 0 output buffers swapped out
     4 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

HDLC is used by default on Cisco serial interfaces. The first important task of troubleshooting serial line problems is to verify that both sides of the link are using the same encapsulation types. Notice the line in the previous output that shows the encapsulation method.

2. Notice the output has the different statistics listed. You cannot effectively troubleshoot if you do not have accurate data returned from the many diagnostic commands. One way to ensure that the data you are analyzing is accurate and directly applies to the problem at hand is to perform the `clear counters serial` *number* command, which resets the interface counters to zero.

```
2600B>clear counters serial 0/0
```

3. Use the `show interface serial 0/0` command to see the counters have been reset:

```
2600B>show interface serial 0/0
```

One of the most important lines in the `show interface` command is the line status. The serial link should display `Serial 0/0 is up, line protocol is up`. The first `up` is related to carrier detect. If you have a connection to a CSU/DSU, then this should appear. The second `up` is keep-alives from the remote router.

4. The `show controllers` command is used to display interface status and whether a cable is connected to the interface. From the 2600B router, use the `show controllers` command to see the cable connections.

   ```
   2600B>show controllers
   ```

   Much of the information in the resulting display will be irrelevant, but you will see that FastEthernet 0/0, serial 0 and serial 1 all have cables attached. The most important aspect to notice is that serial 0 is a DCE cable, which means the clock rate must be used for this interface to appear.

5. The two debug commands that help you troubleshoot serial links are `debug serial interface` and `debug serial packet`. From the 2600B, use the `debug serial interface` command to verify your serial link.

   ```
   2600B>debug serial interface
   2600B>undebug all
   ```

6. From the 2600B router, use `debug serial packet` to verify your serial link.

   ```
   2600B>debug serial packet
   2600B>undebug all
   ```

Lab 7.2: Bugging and Troubleshooting Serial Links

After you have an understanding of the serial tools you can use on Cisco routers to verify your serial links, it is time for you to introduce bugs into your lab and troubleshoot the network.

1. First, verify that your network is currently working.
2. In your lab screen in the program, click the Implement Bugs button.
3. Troubleshoot the network using the tools you learned in Lab 7.1. Do not use a `show running-config` command on either router.

Here are the solutions:

For the 2600B router:

- Enable the serial 0/0 interface with a `no shutdown` command.

- Change the IP address on s0/0 back to 172.16.50.1 255.255.255.0.
- Change the keep-alive on serial 0/0 back to 10.

For the 2600A router:

- Change the keep-alive on serial 0/0 to 10.
- Change the serial 0/0 encapsulation back to HDLC.

Lab 7.3: Configuring Frame Relay

In this lab you will configure Frame Relay between the 2600B and 2600A routers, verify the configuration, and then introduce bugs and troubleshoot Frame Relay. This lab will assume prerequisite knowledge of configuring basic Frame Relay.

Please see Sybex's *CCNA Study Guide* and the *CCNA Virtual Lab* for Frame Relay configuration information.

1. From the 2600B router, configure the Frame Relay encapsulation using DLCI 20. Make the 2600B the Frame Relay switch.

```
2600B>enable
2600B#config t
2600B(config)#frame-relay switching
2600B(config)#interface serial 0/0
2600B(config-if)#encapsulation frame-relay
2600B(config-if)#frame-relay interface-dlci 20
2600B(config-if)#frame-relay intf-type dce
2600B(config-if)#^z
```

2. Configure the 2600A router to use Frame Relay encapsulation on serial interface 0/0 with DCLI 20.

```
2600A>enable
2600A#config t
2600A(config)#interface serial 0/0
2600A(config-if)#encapsulation frame-relay
2600A(config-if)#frame-relay interface-dlci 20
2600A(config-if)#^z
```

3. Verify that the serial links are up and running by using the `show interface` command as well as the `ping` command.

Lab 7.4: Verifying Frame Relay Connectivity

After you have configured Frame Relay, you need to verify the connectivity between the router. Here is a list of the `show` commands that will be covered in this section:

```
show interface
show frame-relay lmi
show frame-relay pvc
show frame-relay map
```

You might have noticed a term you didn't recognize: *LMI (Local Management Interface)*. LMI provides support for keep-alive devices to verify data flow. You will often see this term when dealing with Frame Relay troubleshooting.

1. From the 2600B router, use the `show interface serial 0` command to see the encapsulation and LMI information.

   ```
   2600B#show interface serial 0/0
   ```

2. The relevant Frame Relay terms are listed below:

Frame Relay Term	Meaning
Encapsulation	Cisco routers support two types of Frame Relay: Cisco and IETF.
LMI enq sent	This is the number of LMI enquiries sent.
LMI stat recvd	This is the number of LMI status packets received.
LMI upd recvd	This is the number of LMI updates received.
DTE LMI	This is the status of the DTE Local Management Interface.
LMI enq recvd	This is the number of LMI enquiries received.
LMI stat sent	This is the number of LMI status packets sent.
LMI upd sent	This is the number of LMI updates sent.
LMI DLCI	This is the DLCI number used for LMI. Cisco LMI type uses DLCI 1023. When ANSI is used, the LMI DLCI is 0.

Frame Relay Term	Meaning
LMI type	This is the LMI type used by the interface. The default is Cisco. The other two types are ANSI and ITU-T. The LMI type must match on the router and the Frame Relay switch. Simply put, LMI type must match on the DTE and DCE equipment.

3. The `show frame-relay lmi` command displays LMI-relevant information. The output contains the LMI type, enquiry, update, and status information.

```
2600B#show frame-relay lmi
LMI Statistics for interface Serial0/0 (Frame Relay DCE) LMI
   TYPE = CISCO
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0           Invalid Msg Type 0
  Invalid Status Message 0           Invalid Lock Shift 0
  Invalid Information ID 0           Invalid Report IE Len 0
  Invalid Report Request 0           Invalid Keep IE Len 0
  Num Status Enq. Rcvd 4             Num Status msgs Sent 4
  Num Update Status Sent 0           Num St Enq. Timeouts 2
2600B#
```

4. When you issue the `show frame-relay pvc` command, you get output that contains the LMI status of every DLCI on the router, or you may be more specific and check only certain PVCs.

   There are two types of DLCI usage: local DTE and switched. Things to check for in the output of the command include dropped frames, congestion notifications, and discard-eligible packets.
   Here is a sample output. The data provided includes PVC information. It has the input and output packets for the interface, as well as FECN and BECN packet information. These statistics are available for every DLCI PVC on the router.

```
2600B#show frame-relay pvc

PVC Statistics for interface Serial0/0 (Frame Relay DCE)

                Active      Inactive      Deleted       Static
  Local            1            0            0            0
  Switched         0            0            0            0
  Unused           0            0            0            0
```

```
DLCI = 20, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
         Serial0/0

  input pkts 1           output pkts 0          in bytes 30
  out bytes 0            dropped pkts 0         in FECN pkts 0
  in BECN pkts 0         out FECN pkts 0        out BECN pkts 0
  in DE pkts 0           out DE pkts 0
  out bcast pkts 0       out bcast bytes 0
  pvc create time 00:03:29, last time pvc status changed 00:00:22
```

5. The `show frame-relay map` command contains information about the DLCI numbers and the encapsulation of all Frame Relay interfaces. The status of the interface is indicated with the up or down state found within the parentheses. The next field indicates the type of interface: point-to-point or multipoint.

   The DLCI for the interface and the encapsulation type are also included in the output. Here is the output:

```
2600B#show frame-relay map
Serial0/0 (up): ip 172.16.50.2 dlci 20(0x14,0x440), dynamic,
              broadcast,, status defined, active
```

Lab 7.5: Bugging and Troubleshooting Frame Relay

After you have verified the Frame Relay network in lab 7.4, it is time to introduce bugs into your lab and troubleshoot it.

1. Verify your network is currently working.
2. In your lab screen in the program, click the Implement Bugs button.
3. Use the commands listed in lab 7.4 to troubleshoot the problem.
4. Following are the configuration problems:

   2600B

   - Change the LMI type back to Cisco.
   - Change the keep-alive to 10.

   2600A

   - Configure the frame-relay encap to default, which is Cisco.
   - Configure the interface-dlci number back to 20.

Labs from Chapter 8: Troubleshooting ISDN

This section will have you configure ISDN between the 2600B and 2600A routers, and then verify the configuration. After ISDN is configured between the two routers, ISDN will be used to connect the two routers when the serial link between them fails.

The labs in this section assume a basic knowledge of ISDN. The following switch configurations will be used:

Configuration Element	Setting
ISDN switch-type	basic-ni
Spid1	0835866101
Spid2	0835866301
Dial number	8358661
Encapsulation	PPP
Authentication	CHAP

You will perform the following labs:

- Lab 8.1: Configuring ISDN between the Two Routers
- Lab 8.2: Bringing Up the ISDN Line
- Lab 8.3: Verifying ISDN
- Lab 8.4: Debugging ISDN
- Lab 8.5: Bugging and Troubleshooting ISDN

Read Chapter 8 of Sybex's *CCNP: Support Study Guide* before attempting the labs in this section.

Lab 8.1: Configuring ISDN between the Two Routers

This lab has you configure ISDN on the BRI interfaces of the 2600B and the 2600A routers.

1. Connect to the 2600B router and configure the BRI interface with the ISDN configuration.

```
2600B>enable
2600B#config t
2600B#dialer-list 1 protocol ip permit
2600B(config)#int bri0/0
2600B(config-if)#username 2600A password todd
2600B(config-if)#int bri0/0
2600B(config-if)#encapsulation ppp
2600B(config-if)#ip address 172.16.60.1 255.255.255.0
2600B(config-if)#isdn switch-type basic-ni
2600B(config-if)#isdn spid1 0835866101
2600B(config-if)#isdn spid2 0835866301
2600B(config-if)#ppp authentication chap
2600B(config-if)# dialer string 8358662
2600B(config-if)#dialer-group 1
2600B(config-if)#no shutdown
```

2. Connect to the 2600A router and configure the BRI interface with the ISDN configuration.

```
2600A>enable
2600A#config t
2600A(config)#int bri0/0
2600A(config-if)#username 2600B password todd
2600A(config-if)#int bri0/0
2600A(config-if)#encapsulation ppp
2600A(config-if)#isdn switch-type basic-ni
2600A(config-if)#ip address 172.16.60.2 255.255.255.0
2600A(config-if)#isdn spid1 0835866201
2600A(config-if)#isdn spid2 0835866401
2600A(config-if)#ppp authentication chap
2600A(config-if)#dialer string 8358661
2600A(config-if)#dialer-group 1
2600A(config-if)#no shutdown
```

Lab 8.2: Bringing Up the ISDN Line

This lab has you initiate the ISDN line by configuring the routers with commands that will bring up the line when a failure occurs or the link becomes saturated.

1. Connect to the 2600B router and configure the BRI interface with the ISDN configuration that will enable the connection if a failure of the serial link occurs or if the serial link becomes saturated.

   ```
   2600B(config-if)#interface serial 0/0
   2600B(config-if)#backup interface bri0/0
   2600B(config-if)#backup delay 10 60
   2600B(config-if)#backup load 60 20
   ```

   The backup delay is used to tell the router to wait 10 seconds before bringing up the line, and then drop the line after the serial link is up 60 seconds. The `backup load` command will bring up the ISDN link when the serial link is 60 percent saturated and then drop the link when the load is only 20 percent saturated.

2. Connect to the 2600A router and configure the BRI interface with the ISDN configuration.

   ```
   2600A(config-if)#int s0/0
   2600A(config-if)#backup interface bri0/0
   2600A(config-if)#backup delay 10 60
   2600A(config-if)#backup load 60 20
   ```

3. In your lab screen in the program, click the Implement Bugs button. This will drop the serial link and bring up the ISDN connection.

Once the link is up, go to Lab 8.3 to learn the advanced commands used to verify and troubleshoot the ISDN link.

Lab 8.3: Verifying ISDN

This lab will provide the commands necessary to verify and troubleshoot the ISDN link. The following commands will be used in this lab:

```
ping
show interface bri0/0
show interface bri0/0:n
clear interface bri0/0
```

`show isdn status`

`show dialer`

1. By pinging between routers, you can verify the connection is up and running. For router 2600B, use:

   `2600B#ping 172.16.60.2`

   For Router 2600A, use:

   `2600A#ping 172.16.60.1`

2. Once the `ping` command is successful, use the `show interface bri0` command. It is important for administrators to review the output of the `show interface` command, especially when researching user reports of slow performance. For example, the `txload` and `rxload` parameters provide a strong indication of bandwidth loads. Observe the (spoofing) tag in the following output as well. This indicates that the router is maintaining the link as though it was always active, even though ISDN is dynamic.

   `2600B#show interface bri0/0`

```
BRI0/0 is up, line protocol is up (spoofing)
  Hardware is PQUICC BRI with U interface
  Internet address is 172.16.60.1/24
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliablility 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Last input 00:00:19, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     21 packets input, 152 bytes, 0 no buffer
     Received 11 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     56 packets output, 13082 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     3 carrier transitions
```

3. The `show interface bri0/0:1` or `2` command is used to display a single B channel of the BRI interface. Although this command can be important when isolating an individual B channel problem, the `show interface bri` *n* command usually suffices for the majority of troubleshooting processes.

   ```
   2600B#show interface bri0/0 1
   ```

4. The `clear interface bri` *n* command resets the various counters that are available on the interface and terminates a connection on the interface. The *n* value should equal the port, or port and slot, of the interface. This command is most useful for clearing a call that was activated by a dialer-map or other catalyst, which may be desired when configuring and testing new access lists and other call triggers.

   ```
   2600B#clear int bri0/0
   ```

5. The `show isdn status` command is one of the more significant troubleshooting commands because the output reports not only the status of the interface, but a breakdown of each layer.

   ```
   2600B#show isdn status
   ```

6. The `show dialer` command reports information regarding the DDR connections, including the number dialed, the success of the connection, the idle timers that control the duration of a DDR connection without data packets, and the number of calls that were screened or rejected due to administrative policy. This command is useful for verifying a previous connection or checking the number called.

   ```
   2600B#show dialer
   ```

Lab 8.4: Debugging ISDN

The `debug` commands in ISDN are extremely helpful for researching the causes of problems and resolving them. This section addresses the commands and provides some useful methods for employing them, and it provides some scenarios where such commands may be needed.

The following commands are used in this lab:

```
debug bri

debug isdn q921

debug isdn q931

debug dialer
```

1. The `debug bri` command provides information regarding the B channels of the BRI. Following is an example of the command's output. Note that bandwidth information is also provided. The B channels of the BRI are the data-carrying channels; therefore, an

error in the activation of a B channel prevents data flow. It is also possible for the router to command one B channel to connect while the other B channel fails, which may be due to a misconfigured SPID or other configuration problem. This command provides some insight into this potential problem.

```
2600B#debug bri

Basic Rate network interface debugging is on
2600B#ping 172.16.60.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.60.2, timeout
   is 2 seconds:
.....
Success rate is 0 percent (0/5)
2600B#
*Mar  1 00:38:50.495: dchan tx start
*Mar  1 00:38:50.499: dchan tx intr
*Mar  1 00:38:50.939: dchan tx start
*Mar  1 00:38:50.943: dchan tx intr
```

2. The q.921 protocol addresses Layer 2 of the OSI model and its relationship to ISDN. Information regarding the D channel interface is available via the `debug isdn q921` command. The D channel is always connected in ISDN, and the channel is used for signaling between the switch and local ISDN device. Connections over the B channels cannot occur without signaling commands on the D channel. Administrators should use this command to monitor the proper flow of messages when calls do not connect. It is recommended that a baseline debug be performed and recorded to compare against suspected problem debug output.

```
2600B#debug isdn q921

ISDN Q921 packets debugging is on
2600B#ping 172.16.60.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.60.2, timeout is 2 seconds:
...
*Mar  1 00:42:20.967: ISDN BR0/0: TX ->  RRp sapi = 0  tei = 65 nr = 1
*Mar  1 00:42:21.031: ISDN BR0/0: RX <-  RRf sapi = 0  tei = 65  nr = 1
*Mar  1 00:42:21.407: ISDN BR0/0: TX ->  RRp sapi = 0  tei = 66 nr = 1
*Mar  1 00:42:21.475: ISDN BR0/0: RX <-  RRf sapi = 0  tei = 66  nr = 1..
```

```
Success rate is 0 percent (0/5)
```

3. The q.931 specification addresses Layer 3 of the OSI model for ISDN. Events occurring at Layer 3 may be monitored with the `debug isdn q931` command. In the following output, the two B channels are disconnected.

The output from this command is best compared to a baseline debug captured on a working connection. However, administrators may use the output to verify acknowledgments and messages without a complete understanding of the protocol. There is a great deal of information provided by the following command. However, it can be used to verify the Layer 3 (q.931) setup described earlier in the chapter.

```
2600B#debug isdn q931

[when serial line goes down]
*Mar  1 00:24:22.351: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down

*Mar  1 00:24:23.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
   changed state to down
*Mar  1 00:24:32.355: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to down
*Mar  1 00:24:32.359: %LINK-3-UPDOWN: Interface BRI0/0:2, changed state to down
*Mar  1 00:24:32.407: %LINK-3-UPDOWN: Interface BRI0/0, changed state to up
*Mar  1 00:24:36.659: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0/0, TEI 116
   changed to up
*Mar  1 00:24:36.663: ISDN BR0/0: TX ->  INFORMATION pd = 8  callref = (null)
        SPID Information i = '0835866101'
*Mar  1 00:24:36.935: ISDN BR0/0: RX <-  INFORMATION pd = 8  callref = (null)
        ENDPOINT IDent i = 0x8181
*Mar  1 00:24:36.939: ISDN BR0/0: Received EndPoint ID
*Mar  1 00:24:37.519: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0/0, TEI 118
   changed to up
*Mar  1 00:24:37.519: ISDN BR0/0: TX ->  INFORMATION pd = 8  callref = (null)
        SPID Information i = '0835866301'
*Mar  1 00:24:37.795: ISDN BR0/0: RX <-  INFORMATION pd = 8  callref = (null)
        ENDPOINT IDent i = 0x8381
*Mar  1 00:24:37.799: ISDN BR0/0: Received EndPoint ID

[when serial line goes up]
*Mar  1 00:27:42.135: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar  1 00:27:43.139: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
   changed state to up
2600B#show ip route
```

```
[output cut]
Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.60.0 is directly connected, BRI0/0
C       172.16.50.0 is directly connected, Serial0/0
C       172.16.10.0 is directly connected, FastEthernet0/0
2600B#
*Mar  1 00:28:42.139: %ISDN-6-LAYER2DOWN: Layer 2 for Interface BRI0/0, TEI 116
   changed to down
*Mar  1 00:28:42.139: %ISDN-6-LAYER2DOWN: Layer 2 for Interface BRI0/0, TEI 118
   changed to down
*Mar  1 00:28:42.143: %ISDN-6-LAYER2DOWN: Layer 2 for Interface BR0/0, TEI 116
   changed to down
*Mar  1 00:28:42.143: %ISDN-6-LAYER2DOWN: Layer 2 for Interface BR0/0, TEI 118
   changed to down
*Mar  1 00:28:42.191: %LINK-5-CHANGED: Interface BRI0/0, changed state to standby
   mode
```

4. The `debug dialer` command provides information regarding the cause of a dialing connection and the status of the connection. Note in the following output that an IP packet caused the dial to occur. This information can provide assistance for tuning connections. Administrators frequently do this to limit the use of an ISDN circuit when charged on distance and per-minute tariffs.

```
2600B#debug dialer

*Mar  1 00:19:37.307: %LINK-5-CHANGED: Interface BRI0/0, changed state to standby
   mode
*Mar  1 00:19:37.311: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to down
*Mar  1 00:19:37.315: BRI0/0:1: disconnecting call
*Mar  1 00:19:37.315: %LINK-3-UPDOWN: Interface BRI0/0:2, changed state to down
*Mar  1 00:19:37.319: BRI0/0:2: disconnecting call
```

Lab 8.5: Bugging and Troubleshooting ISDN

This lab will have you introduce bugs and fix the ISDN link.

1. Make sure the lab is configured correctly and that you can run through Lab 8.3.

2. In your lab screen in the program, click the Implement Bugs button.
3. Troubleshoot the ISDN link and fix the problem. Do not use the `show running-config` command on either router. Here are the solutions:

   2600B
   - Configure spid1 to isdn spid1 0835866101.
   - Configure the PPP authentication to CHAP.

   2600A
   - Configure the username 2600B password cisco.
   - Set the int s0/0 to use backup interface bri0/0.
   - Configure the IP address on bri0/0.
   - Configure the encapsulation on bri0/0 to PPP.

Labs from Chapter 9: Troubleshooting Novell Connectivity (IPX)

This section has you configure IPX on the network, introduce bugs, and troubleshoot the network. Internetwork Packet eXchange (IPX) is used on networks to support clients who want to share files with a Novell file server.

This section assumes you already have knowledge of IPX. If not, please see Sybex's *CCNA Study Guide* and *RouterSim CCNA 2.0*. Also make sure the network is configured as in Lab 4.1. The ISDN link should be down and the serial link should be working.

Use the following configuration:

2600B
- FastEthernet0/0: IPX network 10
- Serial 0/0: IPX network 50

2600A
- FastEthernet 0/0: IPX network 10

- Serial 0/0: IPX network 50

This section includes the following lab exercises:

- Lab 9.1: Configuring IPX on the Network
- Lab 9.2: Verifying and Troubleshooting IPX
- Lab 9.3: Debugging IPX
- Lab 9.4: Bugging and Troubleshooting IPX

Read Chapter 9 of Sybex's *CCNP: Support Study Guide* before attempting the labs in this section.

Lab 9.1: Configuring IPX on the Network

This lab will have you set up IPX on the internetwork.

1. From the 2600B router, type the commands to enable IPX routing.

```
2600B>enable
2600B#config t
2600B(config)#ipx routing
2600B(config)#int fastethernet 0/0
2600B(config-if)#ipx network 10
2600B(config-if)#int serial 0/0
2600B(config-if)#ipx network 50
2600B(config-if)#
```

2. From the 2600A router, type the commands to enable IPX routing.

```
2600A>enable
2600A#config t
2600A(config)#ipx routing
2600A(config)#int fastethernet 0/0
2600A(config-if)#ipx network 10
2600A(config-if)#int serial 0/0
2600A(config-if)#ipx network 50
2600A(config-if)#
```

Lab 9.2: Verifying and Troubleshooting IPX

A wide variety of troubleshooting commands are available within the Cisco IOS for resolving IPX networking problems. Although it is important to use all available tools to resolve a network problem—including protocol analyzers, as well as workstation and server applications—most troubleshooting steps are augmented by the IOS commands. As such, there is an emphasis on the following commands and their capabilities to assist as part of an overall problem-resolution strategy:

- `ping` commands
- `show` commands

1. Before you can ping between routers, you need to find the IPX network address of the interfaces. Since these are dynamically assigned using the network number and MAC address of the interface, we must use the CDP commands to find the neighbor's address.

   ```
   2600B#sh cdp neighbor detail
   ```

   Notice in the resulting output that the IP and IPX address of the 2600A router is shown. We can now ping this address.

2. The following example demonstrates an IPX Ping to the 2600A router:

   ```
   2600B#ping ipx 50.0000.30c0.9690
   Type escape sequence to abort.
   Sending 5, 100-byte IPX cisco Echoes to
      200.0000.30c0.9690,    timeout is 2 seconds
   :
   !!!!!
   Success rate is 100 percent (5/5), round-trip
      min/avg/max =    16/20/32 ms
   ```

   Another way to ping the neighbor is with what is called *extended ping*. In the following example, the `Novell Standard Echo` option and `verbose` were selected by using the extended commands:

   ```
   2600B#ping
   Protocol [ip]: ipx
   Target IPX address: 50.0000.30c0.9690
   Repeat count [5]:
   Datagram size [100]:
   Timeout in seconds [2]:
   Verbose [n]: y
   Novell Standard Echo [n]: y
   ```

```
Type escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to
   200.0000.30c0.9690, timeout is 2 seconds:
0 in 20 ms
1 in 20 ms
2 in 20 ms
3 in 16 ms
4 in 20 ms
Success rate is 100 percent (5/5), round-trip
   min/avg/max =    16/19/20 ms
```

You need to figure out the actual IPX addresses of your neighbors. The preceding was an example.

3. The Cisco router's `show` commands provide a great deal of information regarding IPX. This output is available from the `show ipx ?` command. The `show ipx ?` command provides information regarding routing and routing protocols in addition to NetWare servers.

   ```
   2600B#show ipx ?
   ```

4. The `show ipx interface` command provides information on all IPX-configured interfaces. In addition to `show running-config`, this command is useful for locating IPX access lists that may block SAP traffic. The output from this command also provides information about NetBIOS over IPX (type 20) packets, the number of packets sent and received for IPX RIP and SAP, and the status of watchdog and SPX spoof functions.

   ```
   2600B#show ipx interface
   ```

5. The `show ipx route` command is useful for reviewing the state of the NetWare network, and it should be used to confirm that a path exists to the desired resource.

   ```
   2600B#show ipx route
   ```

Notice that only directly connected networks are shown in this output. Our network has no remote networks.

```
[output cut]

No default route known.
```

```
C          10 (NOVELL-ETHER),   Fa0/0
C          50 (FRAME-RELAY),    Se0/0
```

The `show ipx traffic` command reports information about the IPX packets transmitted and received. A sample of this information is presented as follows:

```
2600B#show ipx traffic

System Traffic for 0.0000.0000.0001 System-Name: 2600B
Time since last clear: never
Rcvd:   120 total, 0 format errors, 0 checksum errors, 0 bad
   hop count,
        0 packets pitched, 120 local destination, 0 multicast
Bcast:  115 received, 121 sent
Sent:   123 generated, 0 forwarded
        3 encapsulation failed, 0 no route
SAP:    0 Total SAP requests, 0 Total SAP replies, 0 servers
        0 SAP general requests, 0 ignored, 0 replies
        0 SAP Get Nearest Server requests, 0 replies
        0 SAP Nearest Name requests, 0 replies
        0 SAP General Name requests, 0 replies
        0 SAP advertisements received, 0 sent
        0 SAP flash updates sent, 0 SAP format errors
RIP:    0 RIP requests, 0 ignored, 0 RIP replies, 2 routes
        115 RIP advertisements received, 115 sent
        1 RIP flash updates sent, 0 RIP format errors
Echo:   Rcvd 5 requests, 0 replies
        Sent 0 requests, 5 replies
        0 unknown: 0 no socket, 0 filtered, 0 no helper
        0 SAPs throttled, freed NDB len 0
Watchdog:
        0 packets received, 0 replies spoofed
Queue lengths:
        IPX input: 0, SAP 0, RIP 0, GNS 0
        SAP throttling length: 0/(no limit), 0 nets pending
           lost route reply
        Delayed process creation: 0
EIGRP:  Total received 0, sent 0
        Updates received 0, sent 0
        Queries received 0, sent 0
        Replies received 0, sent 0
        SAPs received 0, sent 0
Trace:  Rcvd 0 requests, 0 replies
        Sent 0 requests, 0 replies
```

Lab 9.3: Debugging IPX

As with other network protocols, there is a wide variety of IPX debug commands available within the Cisco IOS. The debug IPX commands provide the administrator with a means to view Novell traffic in real time as it enters or leaves the router.

The following commands are discussed and shown:

debug ipx routing

debug ipx packet

1. The debug ipx routing command reports all IPX routing processes at the router, including IPX RIP, IPX EIGRP, and NLSP. The first line of its output reports the standard IPX RIP broadcast, whereas the remainder demonstrates the events related to the recovery of an interface configured for IPX.

```
2600B#debug ipx routing events

2600B#debug ipx routing activity
```

2. The debug ipx packet command displays all IPX traffic that enters or leaves the router. Thus, this command can generate a great deal of output, and its use is recommended only with caution.

```
2600B#debug ipx packet
2600B#debug ipx packet
IPX packet debugging is on
2600B#ping ipx 50.00b0.6483.01c0

Type escape sequence to abort.
Sending 5, 100-byte IPXcisco Echoes to
   50.00b0.6483.01c0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
   min/avg/max = 28/31/32 ms
2600B#
*Mar  1 00:19:35.987: IPX: local:50.00b0.6483.2320-
   >50.00b0.6483.01c0 ln=100
tc=
00 pt=01 ds=0002 ss=0002, gw=Se0/0:50.00b0.6483.01c0
*Mar  1 00:19:36.015: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, rcvd
```

```
*Mar  1 00:19:36.019: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, local
*Mar  1 00:19:36.019: IPX: local:50.00b0.6483.2320-
   >50.00b0.6483.01c0 ln=100
tc=
00 pt=01 ds=0002 ss=0002, gw=Se0/0:50.00b0.6483.01c0
*Mar  1 00:19:36.047: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, rcvd
*Mar  1 00:19:36.047: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, local
*Mar  1 00:19:36.051: IPX: local:50.00b0.6483.2320-
   >50.00b0.6483.01c0 ln=100
tc=
00 pt=01 ds=0002 ss=0002, gw=Se0/0:50.00b0.6483.01c0
*Mar  1 00:19:36.079: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, rcvd
*Mar  1 00:19:36.079: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, local
*Mar  1 00:19:36.083: IPX: local:50.00b0.6483.2320-
   >50.00b0.6483.01c0 ln=100
tc=
00 pt=01 ds=0002 ss=0002, gw=Se0/0:50.00b0.6483.01c0
*Mar  1 00:19:36.111: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, rcvd
*Mar  1 00:19:36.111: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, local
```

```
*Mar  1 00:19:36.115: IPX: local:50.00b0.6483.2320-
   >50.00b0.6483.01c0 ln=100
tc=
00 pt=01 ds=0002 ss=0002, gw=Se0/0:50.00b0.6483.01c0
*Mar  1 00:19:36.143: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, rcvd
*Mar  1 00:19:36.143: IPX: Se0/0:50.00b0.6483.01c0-
   >50.00b0.6483.2320 ln=100
tc=
00 pt=02 ds=0002 ss=0002, local
2600B#
```

Lab 9.4: Bugging and Troubleshooting IPX

Once you have the network up and running and you understand the troubleshooting tools, it is time to introduce bugs into the network and then fix it.

1. In your lab screen in the program, click the Implement Bugs button.
2. Run through the commands necessary to find the problems in the network. Do not look at the running-config. You should have found the following:
   - On the 2600B router, the IPX network number on FastEthernet 0/0 was wrong and serial 0/0 was shut down.
   - On the 2600A router, the IPX network number on serial 0/0 was wrong and Fa0/0 was shut down.

Labs from Chapter 11: Troubleshooting Switched Ethernet

This section has you verify and troubleshoot the Catalyst 5000 and 1900 switches in the internetwork. You must have a fundamental understanding of how the Catalyst switches are configured with VLANs and ISL routing before attempting this lab. For more information on Switched Ethernet, VLANs, and ISL routing, see Sybex's *CCNP: Switching Study Guide.* Make sure the network is up and running as described in Lab 4.1.

This series of lab exercises has you create VLANs and connect them using ISL routing through interface FastEthernet 0/0 of the 2600A router. The following configuration will be used:

- VLAN 1: default, used for all switches; Network 172.16.10.0/24 (should already be configured).
- VLAN 2: Sales; HostB is a member of VLAN 2 and is plugged into 1900A interface e0/2.
- VLAN 3: Marketing; HostC is a member of VLAN 3 and is plugged into 1900A interface e0/1.
- The VTP domain is RouterSim with the 5000 being the VTP server.

You will perform the following labs:

- Lab 11.1: Creating VLANs
- Lab 11.2: Routing between VLANs
- Lab 11.3: Verifying and Troubleshooting Switched Ethernet
- Lab 11.4: Bugging and Troubleshooting Switched Ethernet

Read Chapter 11 of Sybex's *CCNP: Support Study Guide* before attempting the labs in this section.

Lab 11.1: Creating VLANs

This lab has you create VLANs 2 and 3 and assign Hosts B and C to the VLANs.

1. From the 5000A switch, create a VTP domain and configure two VLANs. Trunk the ports connected to 1900A and 1900B.

```
5000A>enable
5000A>(enable)set vtp domain RouterSim mode server
5000A>(enable)set vlan 2 name Sales
5000A>(enable)set vlan 3 name Marketing
5000A>(enable)set trunk 2/1 on isl
5000A>(enable)set trunk 2/2 on isl
5000A>(enable)set trunk 1/1 on isl
5000A>(enable)set trunk 1/2 on isl
```

2. Check your configuration on the 5000 switch with the following commands:

```
5000A>(enable)show vtp domain
5000A>(enable)show vlan
5000A>(enable)show trunk
```

3. From the 1900A switch, configure the VTP domain and VLAN assignment and trunk the connection to 5000A.

```
1900A>enable
1900A#config t
1900A#(config)#vtp domain RouterSim
1900A#(config)#vtp client
1900A#(config)#interface ethernet0/2
1900A#(config-if)#vlan-membership static 2
1900A#(config-if)#interface fastethernet 0/26
1900A#(config-if)#trunk on
```

4. From the 1900B switch, configure the VTP domain and VLAN assignment and trunk the connection to 5000A.

```
1900B>enable
1900B#config t
1900B#(config)#vtp domain RouterSim
1900B#(config)#vtp client
1900B#(config)#interface ethernet0/1
1900B#(config-if)#vlan-membership static 3
1900B#(config-if)#interface fastethernet 0/26
1900B#(config-if)#trunk on
```

5. Verify the VLAN and VTP configuration on the 1900 switches.

```
1900B(config-if)#^z
1900B#show vlan
1900B#show vtp
1900B#show trunk a or b
```

Lab 11.2: Routing between VLANs

Lab 11.1 had you create VLANs; however, the devices in each VLAN cannot send packets outside of their VLAN broadcast domain. For each of the hosts to ping each other, routing must be set up.

ISL routing is a Cisco proprietary Inter-VLAN routing protocol that allows multiple VLANs to share information. Once Inter-VLAN routing is set up, all hosts should be able to ping each other.

1. From the 2600 router, configure the Fa0/0 interface with subinterfaces. Use IP addresses 172.16.20.1 and 30.1 for VLANs 2 and 3, respectively.

```
2600A>enable
2600A#config t
2600A(config)#int f0/0
2600A(config-if)#no ip address
2600A(config-if)#int fastethernet 0/0.10
2600A(config-subif)#encap isl 1
2600A(config-subif)#ip address 172.16.10.1
   255.255.255.0
2600A(config-subif)#int fastethernet 0/0.20
2600A(config-subif)#encap isl 2
2600A(config-subif)#ip address 172.16.20.1
   255.255.255.0
2600A(config-subif)#int fastethernet 0/0.30
2600A(config-subif)#encap isl 3
2600A(config-subif)#ip address 172.16.30.1
   255.255.255.0
```

2. Verify that the 2600A can now ping each host.

```
2600A(config-subif)#^z
2600A#ping 172.16.10.6
2600A#ping 172.16.20.2
2600A#ping 172.16.30.2
```

3. Verify that HostA can ping Hosts B and C. Click HostA from the Network Visualizer and type the following:

```
C:>ping 172.16.20.2
C:>ping 172.16.30.2
```

4. For the 2600B router to be able to communicate into VLANs 2 and 3, a routing protocol must be run for the router to propagate the routing table. From the 2600B router, turn on RIP routing.

```
2600B#config t
2600B(config)#router rip
2600B(config-router)#network 172.16.0.0
```

5. Turn on RIP routing on 2600A router as well.

```
2600A#config t
2600A(config)#router rip
2600A(config-router)#network 172.16.0.0
```

Verify that the networks 172.16.20.0 and 172.16.30.0 are in the 2600B routing table. The 2600A router shows them as directly connected.

```
2600B(config-router)#^z
2600B#show ip route
```

6. Now ping to hosts B and C from the 2600B router.

```
2600B#ping 172.16.20.2
2600B#ping 172.16.30.2
```

Lab 11.3: Verifying and Troubleshooting Switched Ethernet

The Catalyst system provides significant diagnostic and administrative tools. These are included in the CLI (command line interface) and CWSI (CiscoWorks for Switched Internetworks). Troubleshooting switched networks frequently includes correlating Layer 2 addressing to Layer 3 and researching Physical layer problems.

1. From the 5000 series switch, the CLI provides a wealth of configuration and diagnostic tools for the administrator. Commands include the set and clear options that are used to configure the switch, and the `show` commands to monitor the current settings. Use the `show ?` command to see the available commands on the 5000 switch.

```
5000A>(enable)show ?
```

2. The `show system` command provides high-level summary information regarding the switch, including the status of power supplies, uptime and administrative settings, and the percentage of traffic on the backplane.

```
5000A>(enable) show system
```

3. The `show port` commands provide specific information about ports or all ports on a module.

```
5000A> (enable) show port ?
```

4. The `show log` command does not report events the same way that a Cisco router does. The command reports significant events, including reboots of all modules, traps, and power supply failures.

```
5000A> (enable) show log
```

5. The `show interface` command reports the IP configuration of the Supervisor module. Although SLIP (serial line interface protocol) connection is configured on sl0, most installations use the in-band sc0 connection. As shown, it belongs to VLAN 1, which always exists on the switch.

```
5000A> (enable) show interface
```

6. The `show config` command is similar to the `show running-config` command on Cisco routers. The command provides all configuration settings on the switch for all modules, with a few exceptions for certain modules, such as the RSM (Route Switch Module).

```
5000A> (enable) show config
```

7. The VLAN Trunk Protocol (VTP) is designed to simplify the introduction of VLANs in multi-switch networks. Within the management domain, a new VLAN is only specified once, and the configuration is propagated throughout the network. The configuration information includes the parameters needed for differing topologies within the switched network. The `show vtp domain` command provides the following status information. Note that VTP updates are sent over VLAN 1 when troubleshooting VTP issues.

```
5000A> (enable)  show vtp domain
```

8. The `show spantree` command reports the status of the spanning tree process for each VLAN, when enabled as follows:

```
5000A> (enable) show spantree
```

9. Cisco switches operate with software that is very similar to the Cisco IOS on routers. This software is stored and may be upgraded in flash memory on the Supervisor module. The `show flash` command reports the space required for the installed software and the version of code.

```
5000A> (enable) show flash
```

10. The `show version` command provides hardware and software version numbers, in addition to memory and system uptime statistics. The output of the command appears as follows:

```
5000A> (enable) show version

WS-C5000 Software, Version McpSW: 4.5(4) NmpSW: 4.5(4)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Oct 18 1999, 10:45:20
MCP S/W compiled on Oct 18 1999, 10:49:13

System Bootstrap Version: 5.1(2)

Hardware Version: 1.8  Model: WS-C5000  Serial #: 005150283

Mod Port Model      Serial #  Versions
--- ---- ---------- --------- --------------------------------
1   2    WS-X5509   005150283 Hw : 1.8
                              Fw : 5.1(2)
                              Fw1: 4.3(1)
                              Sw : 4.5(4)
2   12   WS-X5213   001900981 Hw : 1.2
                              Fw : 1.4
                              Sw : 4.5(4)

       DRAM                    FLASH                    NVRAM
Module Total  Used   Free   Total Used  Free  Total Used Free
------ ------- ------- ------- ------- ------- ------- ----- -
1      32768K 10573K 22195K 8192K 4352K 3840K 256K  113K 143K

Uptime is 0 day, 2 hours, 41 minutes
```

Lab 11.4: Bugging and Troubleshooting Switched Ethernet

After you have completed Labs 11.1 through 11.3, it is time to introduce bugs into the network and troubleshoot it. This lab introduces bugs into both the routers and switches, so pay attention!

1. In your lab screen in the program, click the Implement Bugs button.
2. Run through all the command in Labs 11.1 through 11.3 and use the commands in 11.3 to help you troubleshoot and fix the problems.

Do not view the configs when troubleshooting these problems. Here are the solutions for each piece of equipment:

2600B

- Configure the hostname back to 2600B.
- Enable int s0/0 with a `no shutdown`.
- Enable int f0/0 with a `no shutdown`.

2600A

- Configure the hostname to 2600A.
- Set the keep-alive on int s0/0 to 10.
- Configure RIP routing.

5000A

- Configure the VTP domain.
- Set trunk 2/2 on.

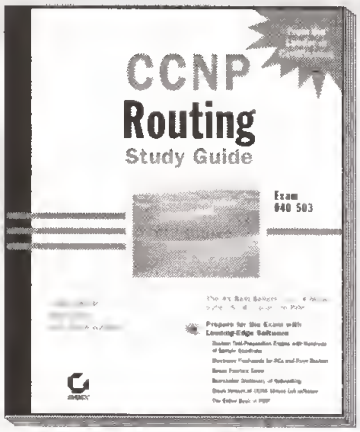
1900A

- Enable int f0/26 to trunk.

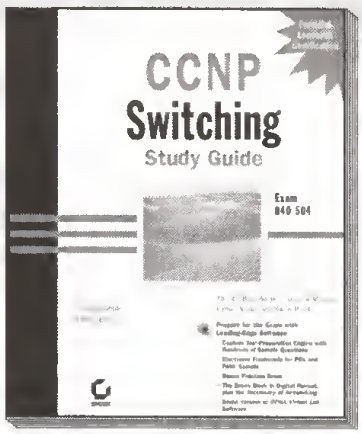
1900B

- Enable int e0/1with vlan-membership 3.

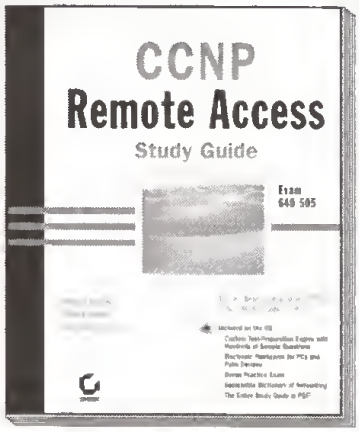
THE COMPLETE CCNP STUDY SOLUTION...



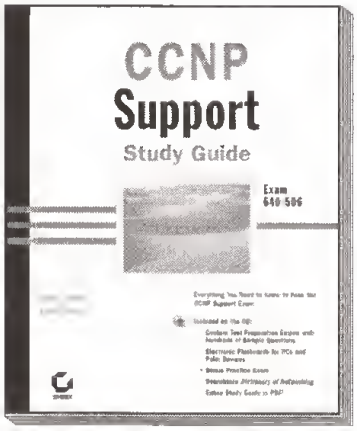
CCNP™: Routing Study Guide
0-7821-2712-6



CCNP™: Switching Study Guide
0-7821-2711-8



CCNP™: Remote Access Study Guide
0-7821-2710-X



CCNP™: Support Study Guide
0-7821-2713-4

Cisco Study Guides from Sybex

- Written by renowned author Todd Lammle and his team of expert authors
- Up-to-date, comprehensive coverage of the Cisco exams
- Hands-on and written labs, plus hundreds of sample questions
- Low-cost alternative to expensive Cisco courses
- Assessment tests and practice exams

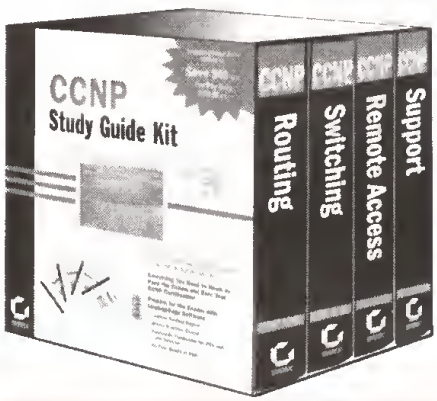
CUTTING-EDGE TEST PREP SOFTWARE ON THE CD

Electronic Flashcards help reinforce key information

Custom Testing Engine simulates Cisco's test format

Bonus Exam assesses knowledge retention

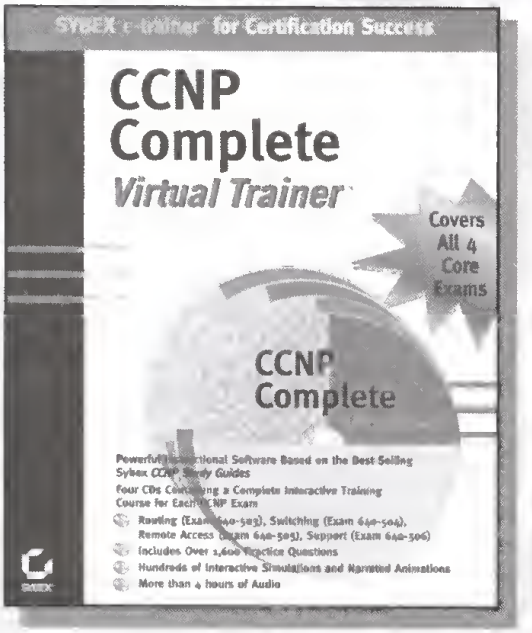
Searchable Ebook allows readers to study anytime, anywhere



CCNP™: Study Guide Kit
0-7821-2718-5

Sybex—The Leader in Certification

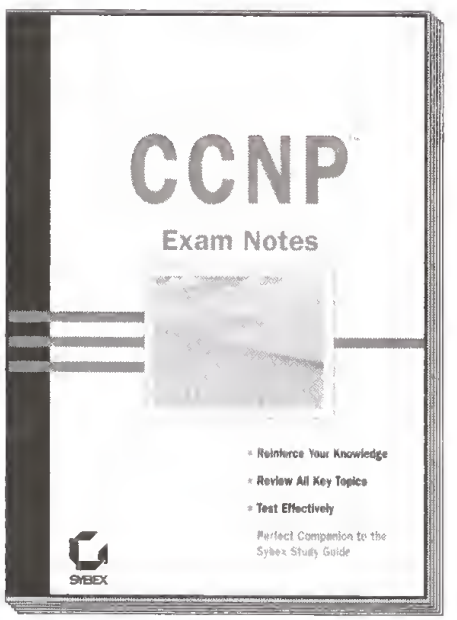
FROM SYBEX!



CCNP™: Complete Virtual Trainer™

0-7821-5011-X

- Based on the content of the best-selling Study Guides, this four-CD *Virtual Trainer* provides in-depth coverage of all the Cisco objectives in a personalized adaptive format.
- Features include a pre-test, which builds a customized study plan, hundreds of sample exam questions, descriptive animations and interactive simulations, audio narration, and detailed reporting features to help you attain your CCNP certification.
- Perfect companion to Sybex's *CCNP Virtual Lab* and *Exam Notes!*



CCNP™: Exam Notes™

0-7821-2919-6

- This comprehensive volume covers all four major areas of the CCNP exams.
- Covers all the Cisco objectives and highlights all key terms, topics, and necessary procedures, plus includes sample questions.
- Perfect companion to the Sybex *CCNP Study Guides*!

www.sybexetrainer.com
certification.sybex.com

SYBEX®

25 Years of Publishing Excellence

Sybex

Barcode 5939735 99385

510 - 523 - 8233

QTTZUUA Ø1ØØØ 8997

CCNP Virtual Lab

ISBN - 0 - 7821 - 5014 - 4

Ver 1.01